UNIVERSIDADE ESTADUAL DE MARINGÁ

CENTRO DE CIÊNCIAS EXATAS

DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

(Mestrado)

Um Conjunto de Informações para Códigos Abelianos

João Vitor Barbosa de Oliveira

Orientadora: Profa. Dra. Fernanda Diniz de Melo Hernandez

Maringá - PR

2024

[1]O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Um Conjunto de Informações para Códigos Abelianos

João Vitor Barbosa de Oliveira

Dissertação apresentada ao Programa de Pós-Graduação em Matemática do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Mestre em Matemática.
Área de concentração: Álgebra

Orientadora: Profa. Dra. Fernanda Diniz de Melo Hernandez

Maringá - PR

2024

Dados Internacionais de Catalogação na Publicação (CIP)
(Biblioteca Setorial BSE-DMA-UEM, Maringá, PR, Brasil)

O482c

Oliveira, João Vitor Barbosa de
Um conjunto de informações para códigos abelianos / João Vitor Barbosa de Oliveira. -- Maringá, 2024.
viii, 87 f. : il.

Orientadora: Profª. Drª. Fernanda Diniz de Melo Hernandez.
Dissertação (mestrado) - Universidade Estadual de Maringá, Centro de Ciências Exatas, Programa de Pós-Graduação em Matemática – Área de Concentração: Álgebra, 2024.

1. Conjunto de informações. 2. Códigos abelianos. 3. Conjunto definidor. 4. Posições de verificação. 5. Decodificação por permutação. I. Hernandez, Fernanda Diniz de Melo, orient. II. Universidade Estadual de Maringá. Centro de Ciências Exatas. Programa de Pós-Graduação em Matemática – Área de concentração: Álgebra. III. Título.

CDD 22.ed. 512.2

Edilson Damasio CRB9-1.123

JOÃO VITOR BARBOSA DE OLIVEIRA

UM CONJUNTO DE INFORMAÇÕES PARA CÓDIGOS ABELIANOS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática tendo a Comissão Julgadora composta pelos membros:

COMISSÃO JULGADORA:

Profa. Dra. Fernanda Diniz de Melo Hernandez - UEM (Presidente)
Prof. Dr. Raul Antonio Ferraz - USP
Profa. Dra. Marinês Guerreiro - UFV
Prof. Dr. Ednei Aparecido Santulo Júnior - UEM

Aprovada em: 11 de março de 2024.
Local de defesa: Bloco F67 – Auditório do Departamento de Matemática.

Agradecimentos

Agradeço primeiramente a minha Mãe por me apoiar em todos os momentos da minha vida, ajudando de todas as maneiras possíveis e impossíveis para que eu pudesse estar aqui.

Agradeço a minha orientadora Profa. Dra Fernanda de Melo Hernandez por me aceitar como seu orientando e por reconhecer minha capacidade.

Aos todos os meus amigos que me apoiaram nos problemas que surgiram ao longo desta dissertação, tanto conceituais quanto pessoais. Em especial, quero agradecer aos amigos Thiago, Luiz e Henrique pelas várias horas de estudos em conjunto e, principalmente, pelos momentos de distração.

Agradeço a todos os professores que de algum modo me ajudaram nessa caminhada.

Aos professores Dr. Ednei Aparecido Santulo Junior, Dra. Marinês Guerreiro e Dr. Raul Antonio Ferraz por aceitarem o convite para participarem da banca e se disporem a ler meu trabalho.

Por fim, agradeço a CAPES pelo apoio financeiro, sem o qual esse trabalho não seria possível.

Resumo

Dado um (n, k) código $\mathcal{C}$, um conjunto de informações para $\mathcal{C}$ é um subconjunto $\mathcal{I} \subset \{1, \ldots, n\}$ de k índices, tal que as palavras código em $\mathcal{C}$ são unicamente determinadas por seus símbolos de informações em $\mathcal{I}$, de modo que a mensagem presente em uma palavra $c \in \mathcal{C}$ está contida exatamente nas posições de $\mathcal{I}$. O objetivo central desse estudo é obter um conjunto de informações para um código abeliano $\mathcal{C}$ arbitrário. Mais especificamente, apresentaremos a construção, dada por Bernal e Simón em [2], de um conjunto de posições de verificações $\Gamma(\mathcal{C})$ cujo complementar é um conjunto de informações. Ao final apresentamos aplicações de como utilizar o conjunto $\Gamma(\mathcal{C})$ para decodificação de códigos abelianos usando o método de decodificação por permutação.

Palavras-chave: Conjunto de informações, códigos abelianos, conjunto definidor, posições de verificação, decodificação por permutação.

Abstract

Given an (n, k) code $\mathcal{C}$ an information set for $\mathcal{C}$ is a subset $\mathcal{I} \subset \{1, \ldots, n\}$ of k indices, such that the code words in $\mathcal{C}$ are uniquely determined by their information symbols in $\mathcal{I}$. In other words, the message present in a word $c \in \mathcal{C}$ is exactly contained in the positions specified by $\mathcal{I}$. The central objective of this study is to obtain an information set for an arbitrary abelian code $\mathcal{C}$. More specifically, we will present the construction, given by Bernal and Simón in [2], of a set of check positions $\Gamma(\mathcal{C})$ whose complement is an information set. Finally, we present applications on how to use the set $\Gamma(\mathcal{C})$ for decoding abelian codes using the permutation decoding method.

Key words: Information sets, abelian codes, defining set, check positions, permutation deconding.

Índice de Notações

$\varnothing$	conjunto vazio
$\mathbb{N}$	conjunto dos números naturais
$\mathbb{Z}$	conjunto dos números inteiros
$\mathbb{Z}_n$	conjunto dos números inteiros módulo n
$\mathbb{F}^*$	elementos não nulos do corpo $\mathbb{F}$
S_n	grupo das permutações de n elementos
$X \subset Y$	X é um subconjunto de Y
$X \dot{\cup} Y$	reunião disjunta
X^c	o conjunto complementar de X
$\|X\|$	cardinalidade do conjunto X
$X \times Y$	produto cartesiano de X por Y
$X \setminus Y$	$\{x \in X \mid x \notin Y\}$
$I \leq A$	I é ideal de A
$[X]$	ideal gerado por X
$A \simeq B$	A isomorfo a B
$Z(A)$	centro do anel A
$Im(f)$	imagem da função f
$\mathbb{K} : \mathbb{F}$	o corpo $\mathbb{K}$ é extensão de $\mathbb{F}$
$Ker(f)$	núcleo de f
$car(\mathbb{F})$	característica do corpo $\mathbb{F}$
$[\mathbb{K} : \mathbb{F}]$	grau de $\mathbb{K}$ sobre $\mathbb{F}$
Id_k	matriz identidade de ordem k
$\langle u, v \rangle$	produto interno de u com v
$\mathbb{F}[X]$	anel de polinômios em X
$\partial(f(X))$	grau do polinômio f
$M_\alpha(X)$	polinômio minimal de α
$\circ(\alpha)$	ordem de α
$C_{(n,q)}(s)$	q-classe ciclotômica de s módulo n
$PAut(\mathcal{C})$	grupo dos automorfismos de permutação de $\mathcal{C}$
$\mathcal{Z}(\mathcal{C})$	conjunto das raízes do código $\mathcal{C}$

$\mathcal{D}(\mathcal{C})$	conjunto definidor do código $\mathcal{C}$
$\overline{\mathcal{D}}(\mathcal{C})$	conjunto restrito de representantes para o código $\mathcal{C}$
$\mathcal{O}(i)$	órbita de i
$cl(\alpha)$	classe dos conjugados de α
$\Gamma(\mathcal{C})$	conjunto de posições de verificação para o código $\mathcal{C}$
$\mathcal{T}(\mathcal{C})$	tensor verificador para o código $\mathcal{C}$

Conteúdo

Introdução

Um código de grupo de comprimento n na álgebra de grupo $\mathbb{F}G$, em que $\mathbb{F}$ é um corpo finito e G é um grupo de ordem n, é um código linear o qual é obtido como imagem de um ideal da álgebra de grupo $\mathbb{F}G$ através de um isomorfismo linear entre $\mathbb{F}G$ e $\mathbb{F}^n$. Foi demonstrado que muitos códigos lineares clássicos são códigos de grupo, daí surge a motivação de estudar os ideais de $\mathbb{F}G$ sob este ponto de vista, veja [12] e[14] por exemplo.

Este trabalho concentra-se em estudar os códigos abelianos, isto é, em estudar os ideais em $\mathbb{F}G$ com G abeliano. Mais especificamente, estudamos a construção, feita por Simón e Bernal em [2], de um conjunto de informações para um código abeliano arbitrário. Tal construção é feita usando a caracterização dos códigos abelianos, descrita na Seção 2.3, a partir de suas raízes.

Os conjuntos de informações são essenciais para descrever os parâmetros de um código linear. Tendo em mãos um conjunto de informações $\mathcal{I}$ podemos obter, por exemplo, a dimensão do código. Também, qualquer palavra código fica completamente determinada por seus valores nas posições em $\mathcal{I}$ denominados de *símbolos de informações*. Deste modo, tais conjuntos são essenciais para os propósitos de codificação e decodificação, sendo assim importante descrever algoritmos eficazes para encontrá-los. Encontrar conjuntos de informações para um código arbitrário pode não ser uma tarefa fácil. Além disso, geralmente, para aplicar um algoritmo de decodificação fixo, existem conjuntos de informação melhores do que outros.

Em [8], Imai apresentou um método para obter conjuntos de informação para códigos cíclicos binários bidimensionais (TDC). Posteriormente, Sakata [18] apresentou um método alternativo para o mesmo propósito. O algoritmo de Imai se baseia na estrutura das raízes do código, enquanto o algoritmo de Sakata é de alguma forma baseado no algoritmo de divisão para polinômios. Seguindo as ideias nos artigos mencionados acima, Chabanne descreveu um método para calcular síndromes via bases de Groebner e,

em seguida, generalizou o procedimento usual de decodificação por permutação (consulte [3]).

Em [2], generaliza-se o método de Imai para códigos abelianos arbitrários. Tal método é baseado no cálculo das cardinalidades de classes ciclotômicas em diferentes extensões do corpo base. Tais classes, assim como suas cardinalidades, são completamente determinadas pela estrutura do conjunto definidor do código (Veja a Definição 2.3.11).

O Capítulo 1 é dedicado à apresentação de alguns resultados que acreditamos ser necessários para uma boa motivação e entendimento desse estudo. Na Secção 1.1, estudamos as extensões de corpos finitos, polinômios minimais e as classes ciclotômicas. Na Seção 1.2, estudamos sucintamente os códigos lineares apresentando os principais assuntos dessa teoria como: métrica de Hamming, matriz geradora e de verificação, conjunto de informações e, por fim, apresentamos o método de decodificação por permutação. Na Seção 1.3, estudamos os códigos cíclicos com ênfase em sua caracterização a partir de suas raízes, esse que é um aspecto motivador para a caracterização dos códigos abelianos.

No Capítulo 2, estudamos os códigos abelianos. Na Seção 2.1 introduzimos o conceito de anel de grupo. Posteriormente, na Seção 2.2, definimos o conceito de código de grupo. Na Seção 2.3, apresentamos a caraterização dos códigos abelianos em termos de suas raízes, também generalizamos alguns conceitos vistos no Capítulo 1 como, por exemplo, os conceitos de conjunto definidor e classes ciclotômicas. Encerrando o capítulo, na Seção 2.4, apresentamos a construção do conjunto de posições, denotado por $\Gamma(\mathcal{C})$, descrita em [2]. Além disso, provamos algumas propriedades relacionadas a $\Gamma(\mathcal{C})$ com o objetivo de provar o teorema principal desse estudo.

Por fim, no Capítulo 3, Seção 3.1, demonstramos que o conjunto $\Gamma(\mathcal{C})$, construído no Capítulo 2, é de fato um conjunto de posições de verificações para um código abeliano qualquer, ou seja, o complementar do conjunto $\Gamma(\mathcal{C})$ é um conjunto de informações para um código abeliano. Também, na Secção 3.2, apresentamos como o conjunto $\Gamma(\mathcal{C})$ pode ser utilizado na decodificação por permutação.

Capítulo 1

Preliminares

Aqui serão apresentadas as notações e resultados fundamentais que sustentarão o desenvolvimento subsequente nos capítulos 2 e 3, delineando assim a estrutura conceitual necessária para a análise detalhada que se seguirá.

Assumiremos que o leitor possui conhecimento de alguns resultados elementares da teoria de grupos, como Teorema de Lagrange, grupos cíclicos e o teorema da decomposição de grupos abelianos finitamente gerados. Também, daremos como conhecidos alguns resultados da teoria de anéis como os conceitos de domínios euclidianos e domínios de ideais principais e alguns resultados básicos relacionados a anéis de polinômios. Recomendamos as referências [4],[9] [16],[17] para consulta desses tópicos.

Na Seção 1.1, iniciamos uma análise da estrutura dos corpos finitos, explorando suas propriedades aritméticas fundamentais e examinando extensões sobre esses corpos. Destacamos, ao final da seção, a importância dos polinômios minimais e a estrutura das classes ciclotômicas, essenciais para a descrição precisa dos polinômios em questão.

Avançando para a Seção 1.2, realizamos uma abordagem concisa, porém abrangente dos códigos lineares, apresentando conceitos cruciais como a métrica de Hamming, Matriz geradora e de verificação e o conjunto de informações. Concluímos a seção introduzindo o método de decodificação por permutação. Para encerrar este capítulo, na Seção 1.3, direcionamos nossa atenção para uma classe específica de códigos lineares: os códigos cíclicos.

1.1 Corpos Finitos e Extensões

Nesta seção, realizaremos uma abordagem introdutória aos corpos finitos, um aspecto essencial para o entendimento dos códigos lineares, dada a abordagem utilizada neste

estudo. Inicialmente, exploraremos a estrutura dos corpos finitos.

1.1.1 Estrutura dos corpos finitos

Denotamos um corpo finito por $\mathbb{F}$. As operações de $\mathbb{F}$ serão denotadas por $+$ e $\cdot$ que denominamos adição e multiplicação, respectivamente. Um exemplo de corpos finitos são os inteiros módulo p, com p primo, denotado por $\mathbb{F}_p := \mathbb{Z}_p$.

Definição 1.1.1. *Seja $\mathbb{F}$ um corpo. Caso exista um inteiro positivo k tal que $kx = \underbrace{x + \ldots + x}_{k \text{ vezes}} = 0$ para cada $x \in \mathbb{F}$, o menor inteiro positivo n tal que, $nx = 0$ para cada $x \in \mathbb{F}$ é chamado **característica** de $\mathbb{F}$ e é indicado por $car(\mathbb{F})$. Caso tal inteiro não exista dizemos que o corpo possui caracterísca zero.*

Quando $\mathbb{F}$ é um corpo finito, então $car(\mathbb{F})$ é sempre um inteiro positivo, na verdade, um número primo. Temos a seguinte propriedade com respeito à característica de um corpo:

Proposição 1.1.2. *Seja $\mathbb{F}$ um corpo finito com característica p e $q = p^r$ para algum inteiro positivo r. Se $a, b \in \mathbb{F}$, temos*

$$(a \pm b)^q = a^q \pm b^q.$$

Demonstração. Veja [6, Proposição 4.3.4]. □

Com base no resultado anterior podemos mostrar a existência de automorfismos não triviais sobre corpos finitos.

Proposição 1.1.3. *Sejam $\mathbb{F}$ um corpo finito, $car(\mathbb{F}) = p$ e $q = p^r$ com r um inteiro, a aplicação:*

$$\begin{array}{rccc} \varphi_q : & \mathbb{F} & \to & \mathbb{F} \\ & x & \mapsto & x^q \end{array}$$

é um automorfismo de corpos.

Demonstração. Veja [13]. □

Definição 1.1.4. *Sejam $\mathbb{F}$ e $\mathbb{K}$ corpos. Dizemos que $\mathbb{K}$ é uma **extensão** de $\mathbb{F}$, e denotamos $\mathbb{K} : \mathbb{F}$, se existe um homomorfismo injetor de anéis $\varphi : \mathbb{F} \to \mathbb{K}$.*

Quando existe um homomorfismo injetor $\varphi : \mathbb{F} \to \mathbb{K}$ entre corpos, isto é, $\mathbb{K} : \mathbb{F}$ então, pelo Teorema do Isomorfismo, $\mathbb{F} \simeq Im(\varphi) \subset \mathbb{K}$. Assim, podemos identificar $\mathbb{F}$ com $Im(\varphi)$, que é um subcorpo de $\mathbb{K}$. Logo, uma extensão $\mathbb{K} : \mathbb{F}$ é, na verdade, uma inclusão $\mathbb{F} \subset \mathbb{K}$ de corpos. Deste modo, por vezes denotaremos $\mathbb{F} \subset \mathbb{K}$ em vez de $\mathbb{K} : \mathbb{F}$. Também, quando $\mathbb{F}$ um corpo finito com $car(\mathbb{F}) = p$, então $\mathbb{F}_p \subset \mathbb{F}$ é uma extensão de corpos.

Observe que toda extensão $\mathbb{F} \subset \mathbb{K}$ da origem a um espaço vetorial, na verdade, à um $\mathbb{F}$-espaço vetorial. De fato, basta considerar sobre $\mathbb{K}$ a operação usual de adição e munir da multiplicação por escalar, definida por:

$$\begin{array}{rccc} \cdot : & \mathbb{F} \times \mathbb{K} & \to & \mathbb{K} \\ & (\lambda, x) & \mapsto & \lambda x \end{array}$$

Assim, tem sentido o seguinte conceito:

Definição 1.1.5. *Seja $\mathbb{F} \subset \mathbb{K}$ uma extensão de corpos com $\mathbb{K}$ finito. Definimos o **grau** de $\mathbb{K}$ sobre $\mathbb{F}$, denotado por $[\mathbb{K} : \mathbb{F}]$, como sendo a dimensão de $\mathbb{K}$ como $\mathbb{F}$-espaço vetorial.*

Observe que, em nosso contexto, o grau de uma extensão é sempre um número inteiro positivo, isto é, as *extensões são finitas*. Com respeito ao grau de uma sucessão de corpos, temos:

Teorema 1.1.6. (Teorema das Torres) *Sejam $\mathbb{K} = \mathbb{K}_1 \subset \mathbb{K}_2 \subset \ldots \subset \mathbb{F}_r$ uma torre de corpos, então:*

$$[\mathbb{K}_r : \mathbb{K}] = [\mathbb{K}_r : \mathbb{K}_{r-1}][\mathbb{K}_{r-1} : \mathbb{K}_{r-2}] \ldots [\mathbb{K}_2 : \mathbb{K}].$$

Demonstração. Veja [19, Teorema 6.4]. □

Também, com o conceito de grau podemos mostrar que todo corpo finito possui ordem p^r para algum inteiro positivo r, isto é, possui uma quantidade potência prima de elementos. Basta notar que, se $car(\mathbb{F}) = p$ então $\mathbb{Z}_p \subset \mathbb{F}$ é uma extensão, logo se $[\mathbb{F} : \mathbb{Z}_p] = r$ então $\mathbb{F}$ e $\mathbb{Z}_p \times \ldots \times \mathbb{Z}_p$, r fatores, são isomorfos como $\mathbb{Z}_p$-espaços vetoriais. Portanto, $|\mathbb{F}| = p^r$. Sintetizemos isto na seguinte proposição.

Proposição 1.1.7. *Seja $\mathbb{F}$ um corpo finito com $car(\mathbb{F}) = p$, então $\mathbb{F}$ possui p^r elementos para algum inteiro positivo r.*

Veremos logo a frente que existe corpo finito de ordem p^r, para todo primo p e para todo inteiro positivo r. Mais ainda, quaisquer dois corpos de mesma ordem são isomorfos. Para tanto é primordial o estudo dos *anéis de polinômios* com coeficientes em um corpo. Por isso introduziremos essa noção agora.

Seja $\mathbb{F}$ um corpo. Consideramos o conjunto de polinômios na variável X com coeficientes em $\mathbb{F}$ como sendo

$$\mathbb{F}[X] = \left\{ \sum_{i=0}^{n} a_i X^i \mid n \in \mathbb{N}; a_i \in \mathbb{F} \right\}$$

Os elementos de $\mathbb{F}[X]$ são denotados por $f(X) = \sum_{i=0}^{n} a_i X^i$ e denominados polinômios. A adição e a multiplicação usual de polinômios munem $\mathbb{F}[X]$ de uma estrutura de anel. Assim, chamamos $\mathbb{F}[X]$ de **anel de polinômios** em X sobre $\mathbb{F}$. Dado um polinômio $f(X) = \sum_{i=0}^{n} a_i X^i \neq 0$, com $a_n \neq 0$, definimos o **grau** de f como sendo n e denotamos $\partial(f(X)) := n$. O anel $\mathbb{F}[X]$ possui um algoritmo de divisão natural induzido pela noção de grau. Isto é, dados $f(X), g(X) \in \mathbb{F}[X]$, existem polinômios $q(X), r(X) \in \mathbb{F}[X]$, unicamente determinados, tais que:

$$f(x) = q(X)g(X) + r(X).$$

De modo que, ou $r(X) = 0$ ou $\partial(r(X)) < \partial(g(X))$. Os polinômios $q(X)$ e $r(X)$ são denominados, respectivamente, de **quociente** e **resto** da divisão euclidiana de $f(X)$ por $g(X)$. Com a divisão euclidiana de polinômios é possível mostrar que $\mathbb{F}[X]$ é um **domínio de ideais principais** (D.I.P), isto é, para cada ideal $I \leq \mathbb{F}[X]$, existe $f(X) \in I$, tal que $I = [f(X)]$. Todo polinômio $f(X) \in \mathbb{F}[X]$ é escrito de modo único como produto de polinômios irredutíveis, isto é, existem $p_1(X), ..., p_r(X) \in \mathbb{F}[X]$ irredutíveis e $\alpha_1, ..., \alpha_r$ inteiros positivos, todos unicamente determinados, tais que:

$$f(X) = p_1^{\alpha_1}(X) \cdot \ldots \cdot p_r^{\alpha_r}(X) \cdot u$$

com $u \in \mathbb{F}$ invertível.

Agora, prosseguiremos de modo a estudar a estrutura dos corpos finitos. Comecemos com um lema.

Lema 1.1.8. *Seja $\mathbb{F}$ um corpo finito com q elementos. Então para cada $\beta \in \mathbb{F}$, $\beta^q = \beta$.*

Demonstração. Veja [10, Lema 3.3.1]. □

Corolário 1.1.9. *Seja $\mathbb{F} \subset \mathbb{K}$ com $|\mathbb{F}| = q$ e considere $\beta \in \mathbb{K}$. Então, $\beta \in \mathbb{F}$ se, e somente se, $\beta^q = \beta$, isto é, $\mathbb{F}$ é o conjunto das raízes do poinômio $X^q - X$.*

Demonstração. Veja [10, Corolário 3.3.2]. □

A seguir apresentaremos três teoremas. O primeiro desses nos mostra que, dado um polinômio $f(X)$ sobre um corpo $\mathbb{F}$, sempre existe uma extensão que contém $\mathbb{F}$ e todas as raízes $f(X)$. O menor corpo com essa propriedade é denominado **corpo de decomposição** de $f(X)$ sobre $\mathbb{F}$ que denotamos por $Gal(f(X), \mathbb{F})$. Os demais teoremas garantem, respectivamente, a unicidade e existência de corpos finitos.

Teorema 1.1.10. *(Kronecker) Sejam $\mathbb{F}$ um corpo e $f(X) \in \mathbb{F}[X]$ um polinômio de grau maior ou igual a 1. Então, existe uma extensão $\mathbb{F} \subset \mathbb{K}$ em que $f(X)$ possui raiz.*

Demonstração. Veja [13, Teorema 11.2]. □

Como consequência do Teorema 1.1.10, dado um polinômio $f(X)$ sobre um corpo $\mathbb{F}$, existe uma extensão $\mathbb{F} \subset \mathbb{E}$ que contém todas as raízes de $f(X)$.

Teorema 1.1.11. *(Unicidade de Copos finitos) Seja $\mathbb{F}$ um corpo finito com $q = p^n$ elementos, então $\mathbb{F}_q = Gal(X^q - X, \mathbb{F}_p)$ é único a menos de isomorfismos.*

Demonstração. Veja [13, Lema 12.2]. □

Teorema 1.1.12. *(Existência de corpos finitos) Sejam p um número primo e n um número inteiro positivo. Então, existe corpo de ordem p^n.*

Demonstração. Veja [13, Teorema 12.1]. □

A partir de agora, sempre que desejarmos explicitar a ordem de um corpo finito $\mathbb{F}$, escreveremos $\mathbb{F}_q$ onde q é a ordem de $\mathbb{F}$. Também, ao longo de todo o texto q será sempre um número inteiro positivo que é potência de um número primo.

Definição 1.1.13. *Diz-se que um elemento α de um corpo finito $\mathbb{F}_q$ é um* ***elemento primitivo*** *se $\mathbb{F}_q = \{0, \alpha, ..., \alpha^{q-1}\}$.*

Se for conveniente, podemos ver os elementos não nulos de um corpo $\mathbb{F}$ como *grupo abeliano multiplicativo*, ou seja, $G := \mathbb{F}\backslash\{0\}$ é um grupo abeliano com a operação de multiplicação de $\mathbb{F}$.

Definição 1.1.14. *Sejam G um grupo finito e $h \in G$, diz-se que a* ***ordem*** *de h é n, e denotamos $n = \circ(h)$, se n é o menor inteiro positivo tal que $h^n = 1$, em que 1 denota o elemento neutro de G. Em particular, o subgrupo gerado por h é dado explicitamente por $H = \{h^r \mid r \in \mathbb{Z}\} = \{1, h, h^2, ..., h^{n-1}\}$.*

Com um pouco de teoria de grupos, é possível ver que, se G é um grupo e $h \in G$ então a ordem de h é um divisor da ordem de G. Tal resultado é conhecido como **Teorema de Lagrange**. Em particular, dado $\alpha \in \mathbb{F}_q^* := \mathbb{F}_q \backslash \{0\}$, $\circ(\alpha) \mid q-1$. Além disso, se G é abeliano, existem elementos de ordem r para cada divisor r da ordem de G.

O próximo resultado assegura a existência de elementos primitivos para qualquer que seja o corpo $\mathbb{F}_q$.

Teorema 1.1.15. *O grupo $\mathbb{F}_q^*$ é um grupo cíclico. Em particular, todo corpo finito $\mathbb{F}_q$ possui elementos primitivos.*

Demonstração. Veja [9, Teorema 22.10]. □

O seguinte teorema caracteriza todos os subcorpos de um corpo $\mathbb{F}_q$.

Teorema 1.1.16. *O corpo $\mathbb{F}_q$, com $q = p^n$ e p primo, contém um subcorpo $\mathbb{K}$ de ordem p^m se, e somente se, $m \mid n$. Nesse caso, existe um único subcorpo com a propriedade de que $m \mid n$, seus elementos são precisamente as raízes em $\mathbb{F}$ do polinômio $X^{p^m} - X$.*

Demonstração. Veja [13, Teorema 12.2]. □

1.1.2 Polinômios Minimais

Seja $\mathbb{F}_{q^r} \subset \mathbb{F}_{q^t}$ uma extensão de corpos. Sabemos que todo elementos $\alpha \in \mathbb{F}_{q^t}$ é raiz do polinômio mônico $X^{q^t} - X \in \mathbb{F}_{q^r}[X]$.

Definição 1.1.17. *Seja $\mathbb{F}_{q^r} \subset \mathbb{F}_{q^t}$ uma extensão de corpos e $\alpha \in \mathbb{F}_{q^t}$. Existe um polinômio mônico de menor grau $M_\alpha(X) \in \mathbb{F}_{q^r}$ que se anula em α denominado* ***polinômio minimal*** *de α sobre $\mathbb{F}_{q^t}$.*

Teorema 1.1.18. *Sejam $\mathbb{F}_{q^r} \subset \mathbb{F}_{q^t}$ uma extensão e $\alpha \in \mathbb{F}_{q^t}$, temos:*

1. *$M_\alpha(X)$ é irredutível sobre $\mathbb{F}_{q^r}$;*

2. *Se* $g(X) \in \mathbb{F}_{q^r}$ *é tal que,* $g(\alpha) = 0$*, então* $M_\alpha(X) \mid g(X)$*;*

3. M_α *é único, isto é, existe um único polinômio mônico sobre* $\mathbb{F}_{q^r}$ *de menor grau tal que* α *é raiz.*

Demonstração. Veja [7, Teorema 3.7.1]. □

Definição 1.1.19. *Sejam* $\mathbb{F} \subset \mathbb{K}$ *uma extensão e* $\alpha \in \mathbb{F}$*, definimos o corpo de* ***adjunção*** *de* $\mathbb{F}$ *a* α*, denotado por* $\mathbb{F}(\alpha)$*, como sendo o menor subcorpo de* $\mathbb{K}$ *que contém* $\mathbb{F}$ *e* α*, isto é,* $\mathbb{F}(\alpha)$ *é a interseção de todos os subcorpos de* $\mathbb{K}$ *que contém* $\mathbb{F}$ *e* α*.*

Lema 1.1.20. *Sejam* $\mathbb{F} \subset \mathbb{K}$ *uma extensão e* $\alpha \in \mathbb{K}$*. Então,* $\mathbb{F} \subset \mathbb{F}(\alpha)$ *é uma extensão com grau é igual ao grau de* $M_\alpha(X)$*.*

Demonstração. Veja [13, Lema 11.4] □

Teorema 1.1.21. *Seja* $f(X)$ *um polinômio mônico irredutível de grau* r *sobre* $\mathbb{F}_q$*. Então:*

1. *Todas as raízes de* $f(X)$ *estão em* $\mathbb{F}_{q^r}$*. Além disso, se* $\mathbb{F}_q \subset \mathbb{K}$ *é uma extensão que contém algum raiz de* $f(X)$ *então* $\mathbb{K}$ *contém todas as raízes de* $f(X)$*;*

2. $f(X) = \prod_{i=1}^{r}(X - \alpha_i)$*, para convenientes* $\alpha_i \in \mathbb{F}_{q^r}$*;*

3. $f(X) \mid X^{q^r} - X$*.*

Demonstração. Veja [7, Teorema 3.7.2]. □

Em particular, quando tomamos $f(X) = M_\alpha(X)$, obtemos o seguinte:

Teorema 1.1.22. *Sejam* $\mathbb{F}_{q^t}$ *uma extensão de* $\mathbb{F}_q$ *e* $\alpha \in \mathbb{F}_{q^t}$*, então:*

1. $M_\alpha(X) \mid X^{q^t} - X$*,*

2. $M_\alpha(X)$ *tem todas as raízes distintas em* $\mathbb{F}_{q^t}$*.*

3. *O grau de* M_α *divide* t*.*

4. $X^{q^t} - X = \prod_\alpha M_\alpha(X)$*, onde* α *percorre um subconjunto que enumera os polnômios mínimas de cada elemento* $\mathbb{F}_{q^t}$ *exatamente uma vez, isto é, se* $M_\alpha = M_\beta$ *então* M_α *aprece apenas uma vez na decomposição,*

5. $X^{q^t} - X = \prod_f f(X)$, *onde* f *percorrendo todos os polinômios mônicos irredutíveis cujo grau divide* t.

Demonstração. Veja [7, Teorema 3.7.3]. □

1.1.3 Classes Ciclotômicas

Definição 1.1.23. *Diz-se que elementos* $\alpha, \beta \in \mathbb{F}_{q^t}$ *são* $\mathbb{F}_q$-***conjugados*** *ou, simplesmente,* ***conjugados*** *se* $M_\alpha(X) = M_\beta(X)$. *Além disso, denotamos por* $cl(\alpha)$ *o conjunto de todos os* $\mathbb{F}_q$*-conjugados de* α *que chamamos de* $\mathbb{F}_q$-***classe*** *de* α.

É natural ver que a relação definida por:

$$\alpha, \beta \in \mathbb{F}_{q^t}, \alpha \sim \beta \iff \beta \in cl(\alpha)$$

é uma relação de equivalência. Veremos posteriormente que é importante conhecer todos os conjugados de um certo elemento $\alpha \in \mathbb{F}_{q^t}$ ou, de maneira equivalente, conhecer todas as raízes de $M_\alpha(X)$ as quais, pelo Teorema 1.1.22, estão em $\mathbb{F}_{q^t}$. A seguinte proposição nos auxiliará a alcançar esse objetivo.

Proposição 1.1.24. *Seja* $f(X) \in \mathbb{F}_q[X]$ *e* α *uma raiz de* $f(X)$ *em alguma extensão* $\mathbb{F}_q \subset \mathbb{F}_{q^t}$, *então* $f(X)^q = f(X^q)$ *e* α^q *é raiz de* $f(X)$.

Demonstração. Veja [7, Teorema 3.7.4]. □

Aplicando a Proposição 1.1.24 obtemos que $\alpha, \alpha^q, \alpha^{q^2} \ldots$ são raízes de $M_\alpha(X)$. Além disso, existe um inteiro positivo r tal que essa sequência para e $\alpha^{q^r} = \alpha$. De fato, pela estrutura dos corpos finitos, existe um inteiro positivo r tal que $\alpha^{q^r} = \alpha$. Suponha que r é o menor inteiro positivo possível e veja que $\alpha, \alpha^q, \ldots, \alpha^{q^{r-1}}$ são dois a dois distintos.

Agora, considere $\gamma \in \mathbb{F}_{q^t}$ um elemento primitivo. Então um inteiro positivo s tal que, $\alpha = \gamma^s$. Assim, $\alpha^{q^r} = \alpha$ se, e somente se, $\gamma^{sq^r} = \gamma^s$ se, e somente se, $\gamma^{sq^r - s} = 1$ o que ocorre se, e somente se, $sq^r \equiv s (mod\ q^t - 1)$.

Proposição 1.1.25. *Sejam* $a, b \in \mathbb{Z}_{q^t-1}$, *a relação:*

$$a \sim b \iff \exists i \in \mathbb{Z} : a \equiv bq^i (mod\ q^t - 1)$$

é uma relação de equivalência.

Demonstração. De fato, a relação $\sim$ é reflexiva, pois $a \equiv aq^0 \pmod{q^t-1}$. Para a propriedade simétrica, suponha $a \sim b$, então existe $i \in \mathbb{Z}$ tal que, $a \equiv bq^i (mod\ q^t-1)$. Como $mdc(q, q^t-1) = 1$ que q é invertível módulo q^t-1 implicando que q^i também é. Assim, $aq^{-i} \equiv b (mod\ q^t-1)$ e $b \sim a$. Finalmente, vejamos que $\sim$ é transitiva. Para tanto, suponha que existam $i, j \in \mathbb{Z}$ tais que $a \equiv bq^i (mod\ q^t-1)$ e $b \equiv cq^j = (mod\ q^t-1)$, então $a \equiv cq^{i+j}$. Portanto, $\sim$ é uma ralação de equivalência sobre $\mathbb{Z}_{q^t-1}$. □

Com base nisso definimos

Definição 1.1.26. *A q-**classe ciclotômica** de um inteiro s módulo q^t-1 é definida como sendo o conjunto:*

$$\begin{aligned} C(s) &= \{sq^i (mod\ q^t-1) \mid i \in \mathbb{Z}\} \subset \mathbb{Z}_{q^t-1} \\ &= \{s, sq, \ldots, sq^{r-1}\} \subset \mathbb{Z}_{q^t-1} \end{aligned}$$

em que r é o menor inteiro positivo tal que $sq^r \equiv s (mod\ q^t-1)$.

Como consequência da Proposição 1.1.25 temos o seguinte:

Corolário 1.1.27. *O conjunto de todas as q-classes ciclotômicas módulo q^t-1 determinam uma partição de $\mathbb{Z}_{q^t-1}$.*

Definição 1.1.28. *Diz-se que um conjunto $\{C(s_1), \ldots, C(s_k)\}$ de q-classes ciclotômicas módulo q^t-1 é um conjunto **completo de representantes** se $\mathbb{Z}_{q^t-1} = \bigcup_{j=1}^{k} C(s_i)$ e $C(s_u) \bigcap C(s_v) = \varnothing$ sempre que $1 \leq u \neq v \leq k$.*

Proposição 1.1.29. *Sejam $\alpha \in \mathbb{F}_{q^t}$ e $M_\alpha(X)$ o polinômio minimal de α sobre $\mathbb{F}_q$. Se $\alpha = \gamma^s$, com γ um elemento primitivo de $\mathbb{F}_{q^t}$, então $\partial(M_\alpha(X)) = |C(s)|$. Além disso,*

$$M_{\gamma^s} = \prod_{i \in C(s)} (X - \gamma^i).$$

Demonstração. Considere $r = \partial(M_\alpha(X))$. Note que, se provarmos que os elementos $\alpha = \gamma^s, \gamma^{sq}, \ldots, \gamma^{sq^{r-1}}$ são dois a dois distintos, teremos o desejado, pois isso implicaria $|C(s)| \geq r$. Por outro lado, $|C(s)| \leq r$, pois todos os elementos da forma γ^i com $i \in C(s)$ são raízes de $M_\alpha(X)$ que são no máximo r. Assim, $|C(s)| = r$ como desejamos. De fato, considere o polinômio

$$g(X) = (X - \alpha)(X - \alpha^q) \cdot \ldots \cdot (X - \alpha^{q^{r-1}})$$

Afirmo que $g(X) \in \mathbb{F}_q[X]$. Para ver isso, note primeiramente que $\alpha = \alpha^{q^r}$, pois $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^r}$, implicando que:

$$\begin{aligned} g(X^q) &= (X^q - \alpha)(X^q - \alpha^q) \cdot \ldots \cdot (X^q - \alpha^{q^{r-1}}) \\ &= (X^q - \alpha^{q^r})(X^q - \alpha^q) \cdot \ldots \cdot (X^q - \alpha^{q^{r-1}}) \\ &= [(X - \alpha^{q^r-1})(X - \alpha) \cdot \ldots \cdot (X - \alpha^{q^{r-2}})]^q \\ &= g(X)^q. \end{aligned}$$

Deste modo, se $g(X) = a_0 + a_1X + \ldots + X^r$, então $a_i^q = a_i$ para cada i implicando que $a_i \in \mathbb{F}_q$. Logo, $g(X) \in \mathbb{F}_q[X]$. Como $g(\alpha) = 0$ e $g(X)$ é mônico e possui o mesmo grau que $M_\alpha(X)$ segue-se que, $M_\alpha(X) = g(X)$. Finalmente, como as raízes de $M_\alpha(X)$ são simples, temos o desejado. □

Observação 1.1.30. Convém observar que a $\mathbb{F}_q$-classe de um elemento $\gamma^s = \alpha \in \mathbb{F}_{q^t}$ é exatamente $cl(\alpha) = \{\gamma^i \mid i \in C(s)\}$ com γ um elemento primitivo de $\mathbb{F}_{q^t}$.

1.2 Códigos Lineares

Os códigos lineares são uma classe de códigos de correção de erros utilizados na teoria da informação e na codificação de dados. Eles foram desenvolvidos por Claude Shannon na década de 1940, enquanto ele estava trabalhando na Bell Labs. Shannon é frequentemente considerado o pai da teoria da informação e seu trabalho fundamental influenciou significativamente o campo da comunicação digital. A principal ideia é utilizar propriedades algébricas para facilitar a detecção e correção de erros.

Ao longo do tempo, várias extensões e generalizações dos códigos lineares foram desenvolvidas para atender a diferentes requisitos de aplicações práticas. Eles desempenham um papel crucial em sistemas de comunicação, armazenamento de dados e transmissão de informação digital, proporcionando confiabilidade na presença de erros.

Nesta seção, apresentaremos sucintamente o conceito de código linear, acompanhado dos elementos fundamentais dessa estrutura, como matriz geradora, matriz de verificação, métrica de Hamming e peso do código. No entanto, o foco principal reside no estudo dos códigos cíclicos a partir de suas raízes. O estudo realizado no Capítulo 2 sobre códigos abelianos representa, em certo sentido, uma generalização natural dos códigos cíclicos, em

que estendemos o conceito de classe ciclotômica. Além disso, introduziremos o conceito de *conjunto de informações*, que constitui o tema central deste estudo.

1.2.1 Métrica de Hamming

Comecemos com a definição de Código Linear.

Definição 1.2.1. *Diz-se que um subconjunto próprio $\mathcal{C} \subset \mathbb{F}^n$ é um (n,k)-**código linear** se $\mathcal{C}$ for um $\mathbb{F}$-subespaço vetorial de $\mathbb{F}^n$ de* dimensão k. *Ainda, dizemos que n é o **comprimento** do código, $\mathbb{F}$ é o **alfabeto**, os elementos de $\mathbb{F}^n$ são ditas **palavras** e um elemento do $\mathcal{C}$ é dito **palavra-código**.*

Geralmente, denotamos os vetores (ou as palavras) em $\mathbb{F}^n$ por $(a_1, a_2, \ldots, a_n)$ ou, quando conveniente, $a_1 a_2 \ldots a_n$.

Definição 1.2.2. *Dadas duas palavras $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n)$ em $\mathbb{F}^n$, definimos a **distância de Hamming** entre x e y ao número de coordenadas em que estes elementos diferem, isto é,*

$$d(x,y) := |\{i \mid x_i \neq y_i 1, 1 \leq i \leq n\}|.$$

Não é uma tarefa difícil verificar que a função d realmente define uma métrica, ou seja, que d satisfaz as seguintes propriedades:

d1. $d(x,y) \geq 0$, para quaisquer $x, y \in \mathbb{F}^n$;

d2. Se $x \neq y$, então $d(x,y) > 0$ para quaisquer $x, y \in \mathbb{F}^n$;

d3. $d(x,y) = d(y,x)$, para quaisquer $x, y \in \mathbb{F}^n$;

d4. $d(x,z) \leq d(x,y) + d(y,z)$, para quaisquer $x, y, z \in \mathbb{F}^n$.

Definição 1.2.3. *Dada uma palavras $x \in \mathbb{F}$, define-se o **peso** de x por*

$$\omega(x) = |\{i \mid x_i \neq 0\}| = d(x,0).$$

*Também, dado um código linear $\mathcal{C}$ a **distância mínima** de $\mathcal{C}$ é o inteiro*

$$d(\mathcal{C}) := min\{d(x,y) \mid x, y \in \mathcal{C}\} = min\{\omega(x) \mid x \in \mathcal{C} \backslash \{0\}\}.$$

Observação 1.2.4. Convém observar que se pode definir o conceito de distância mínima em um contexto mais geral, isto é, mo qual o código $\mathcal{C}$ considerado não possui estrutura algébrica. Nesse caso, não vale, em geral, a igualdade $d(\mathcal{C}) := min\{d(x,y) \mid x,y \in \mathcal{C}\} = min\{\omega(x) \mid x \in \mathcal{C}\backslash\{0\}\}$ essa que segue da estrutura de subespaço vetorial do $\mathcal{C}$.

É comum se referir ao um código linear $\mathcal{C}$ a partir dos seus *parâmetros*, isto é, como sendo um (n,k,d)-código linear em que d é a distância mínima ou, equivalentemente, o peso de $\mathcal{C}$, n é o comprimento das palavras e k é a dimensão de $\mathcal{C}$.

Dado um número real λ, definimos a *parte inteira* de λ, $[\lambda]$, o maior inteiro menor ou igual a λ. O próximo resultado revela a importância do conceito de distância mínima de um código.

Teorema 1.2.5. *Seja $\mathcal{C}$ um (n,k,d)-código linear, se*

$$\kappa = \left[\frac{d-1}{2}\right].$$

Então é possível detectar até $d-1$ erros e corrigir até κ erros.

Demonstração. Veja [10, Teorema 2.5.10]. □

Definição 1.2.6. *Dado um código linear $\mathcal{C}$ com distância mínima d, o número inteiro*

$$\kappa = \left[\frac{d-1}{2}\right]$$

chama-se ***capacidade de correção*** *de $\mathcal{C}$.*

1.2.2 Gerando Códigos Lineares

Existem algumas maneiras de obter um (n,k)-código linear $\mathcal{C}$. Uma dessas é a partir de *transformações lineares*. Para $\mathcal{C}$ um subespaço vetorial de $\mathbb{F}^n$ de dimensão k, temos que $\mathbb{F}^k$ e $\mathcal{C}$ são isomorfos como $\mathbb{F}$-espaços vetoriais. Assim, dar um código linear $\mathcal{C}$ de comprimento n equivale a exibir um monomorfismo linear (transformação linear injetiva) $T : \mathbb{F}^k \to \mathbb{F}^n$ e definir $\mathcal{C} = T(\mathbb{F}^k)$. Nessas condições, o espaço $\mathbb{F}^k$ é denominado **código-fonte** e T é chamada de **codificação**. Porém, existe outro modo de descrever um código $\mathcal{C}$ por meio do núcleo de uma transformação linear. Vejamos como fazer isto. Primeiramente, tome $\mathcal{C}'$ o complemento de $\mathcal{C}$ em $\mathbb{F}^n$, isto é, $\mathcal{C}'$ é tomado de modo que $\mathcal{C} \oplus \mathcal{C}' = \mathbb{F}^n$. Considere a

transformação linear

$$\begin{array}{rccc} \varphi: & \mathcal{C}\oplus\mathcal{C}' & \to & \mathbb{F}^{n-k} \\ & u+v & \mapsto & v \end{array} \tag{1.1}$$

Note que $x = u + v \in \ker(\varphi)$ se, e somente se, $\varphi(x) = v = 0$ ou, equivalentemente, $x \in \mathcal{C}$. Portanto, $\ker(\varphi) = \mathcal{C}$. Note que, para verificar se uma palavra $v \in \mathbb{F}_q^n$ pertence a $\mathcal{C}$, basta verificar se $\varphi(v) = 0$.

Também, podemos obter códigos a partir de matrizes. De fato, se $\mathcal{C}$ é um código linear de dimensão k, então podemos obter uma base $\mathscr{B} = \{v_1, ..., v_k\}$ que gera $\mathcal{C}$. Também, sendo os elementos de $\mathscr{B}$ n-uplas ordenadas em $\mathbb{F}_q^n$, podemos escrever os vetores de$\mathscr{B}$ como sendo linhas de uma matriz

$$G = \begin{pmatrix} v_{11} & \dots & v_{1n} \\ \vdots & \ddots & \vdots \\ v_{k1} & \dots & v_{kn} \end{pmatrix}_{k\times n}$$

com $v_i = (v_{i1}, \dots, v_{in})$ para $i = 1, \dots, k$. Observe que tal matriz G não é necessariamente única, visto que depende da escolha da base $\mathscr{B}$. Deste modo, dado qualquer vetor $\lambda = (\lambda_1, \dots, \lambda_k) \in \mathbb{F}_q^k$ temos $\lambda \cdot G \in \mathcal{C}$. A recíproca também é verdadeira, isto é, $c \in \mathcal{C}$ se, e somente se, existe $\lambda \in \mathbb{F}_q^k$ tal que $c = \lambda G$.

Definição 1.2.7. *Nas condições acima dizemos que a matriz G é uma* ***matriz geradora*** *de $\mathcal{C}$ associada à base $\mathscr{B}$.*

Observação 1.2.8.

1. Se G é uma matriz geradora de um código $\mathcal{C}$, então a aplicação

$$\begin{array}{rccc} T: & \mathbb{F}_q^k & \to & \mathbb{F}_q^n \\ & x & \mapsto & xG \end{array}$$

é uma transformação linear e $T(\mathbb{F}_q^k) = \mathcal{C}$.

2. Note que se $\mathcal{C}$ é um (n, k)-código linear, então $\mathcal{C}$ possui exatamente q^k palavras. Isso ocorre, pois cada elemento $\lambda \in \mathbb{F}_q^k$ dá origem a um único elemento $\lambda G \in \mathcal{C}$. Como $\mathbb{F}_q$ possui q elementos e $\lambda = (\lambda_1, \dots, \lambda_k)$, com $\lambda_i \in \mathbb{F}_q$, temos q^k possibilidades para a escrita de λ.

Lembremos que uma base em um espaço vetorial pode ser obtida de uma outra qualquer através de uma sequência de operações do tipo

- Permutar dois elementos da base.
- Multiplicar um elemento da base por um escalar não nulo.
- Substituir um vetor da base por ele mesmo somado com um múltiplo escalar de outro vetor da base.

Assim, duas matrizes geradoras de um mesmo código linear $\mathcal{C}$ podem ser obtidas uma da outra por uma sequência de operações do tipo:

L1. Permutar duas linhas;

L2. Multiplicar uma linha por um escalar não nulo.;

L3. Adição de um múltiplo escalar de uma linha a outra.

Definição 1.2.9. *Diremos que uma matriz geradora G está sob a* forma padrão*, quando for possível escrever*

$$G = (Id_k|A)$$

com Id_k é a matriz identidade $k \times k$ e $A = (a_{ij})_{k\times(n-k)}$.

Ter uma matriz geradora sob a forma padrão é de grande importância, pois os primeiros k símbolos do vetor recebido formam o que denominamos de *símbolos de informações*, isto é, a restrição desse vetor às k primeiras entradas é a decodificação da palavra-código. As demais $n - k$ posições são chamadas de *redundâncias* ou *posições de verificação.*

Observação 1.2.10. Dado um código $\mathcal{C}$, nem sempre é possível encontrar uma matriz geradora para $\mathcal{C}$ sob a forma padrão, por exemplo, o código em $\mathbb{F}_2^5$ de matriz geradora

$$G = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

não possui matriz geradora sob a forma padrão $(Id_2|A_{3\times2})$. Com efeito, efetuando qualquer uma das operações (L1), (L2) ou (L3) sempre obtemos uma matriz da forma $(0_{2\times2}|A_{3\times2})$.

A seguir definiremos o conceito de *códigos equivalentes por permutação*, esse que nos ajuda a contornar o problema de nem sempre conseguir obter uma matriz sob a forma padrão.

Definição 1.2.11. *Dados códigos lineares $\mathcal{C}$ e $\tilde{\mathcal{C}}$ em $\mathbb{F}^n$, diz-se que $\mathcal{C}$ e $\tilde{\mathcal{C}}$ são* ***equivalentes por permutação*** *ou, simplesmente,* ***equivalentes****, se existir $\sigma \in S_n$, tal que a isometria linear, que ainda denotamos por σ, definida por:*

$$\begin{array}{rccc} \sigma: & \mathbb{F}^n & \to & \mathbb{F}^n \\ & (x_1, \ldots, x_n) & \mapsto & (x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \end{array}$$

é tal que $\sigma(\mathcal{C}) = \tilde{\mathcal{C}}$. Além disso, dizemos que σ é um ***automorfismo induzido por permutação****, ou, simplesmente,* ***automorfismo de permutação****.*

Note, realmente, que σ é uma isometria, isto é, $d(x, y) = d(\sigma(x), \sigma(y))$, para quaisquer $x, y \in \mathbb{F}^n$ em que d denota a métrica de Hamming. Em particular, se $\mathcal{C}$ e $\tilde{\mathcal{C}}$ são equivalentes, então $\mathcal{C} \simeq \tilde{\mathcal{C}}$ como $\mathbb{F}$-espaços vetoriais e, além disso, os parâmetros do código são invariantes por automorfismos de permutações. Para mais detalhes, consulte [6, Seções 1.3 e 5.1]. Sintetizemos essas informações no seguinte teorema.

Teorema 1.2.12. *Sejam $\mathcal{C}$ e $\tilde{\mathcal{C}}$ códigos lineares equivalentes sobre $\mathbb{F}^n$. Dado $c \in \mathcal{C}$ temos que, $\omega(c) = \omega(\sigma(c))$. Além disso, $\mathcal{C}$ possui parâmetros (n, k, d) se, e somente se, $\tilde{\mathcal{C}}$ também possui parâmetros (n, k, d).*

Como a noção de códigos equivalentes sugere, temos:

Proposição 1.2.13. *Seja $\mathcal{S}$ a família de todos os subespaços vetoriais de $\mathbb{F}_q^n$, a relação sobre $\mathcal{S}$, definida por:*

$$\mathcal{C} \sim \tilde{C} \iff \mathcal{C} \text{ é equivalente a } \tilde{\mathcal{C}}$$

é uma relação de equivalência.

Demonstração. Segue dos seguintes fatos: i_d é uma isometria linear, $i_d \in S_n$ a identidade, a inversa de um isometria linear é ainda uma isometria linear e composições de isometrias lineares é também uma isometria linear. □

O próximo resultado assegura a existência de códigos equivalentes com matriz sob a forma padrão.

Teorema 1.2.14. *Todo código linear $\mathcal{C}$ possui um código equivalente $\tilde{C}$ com matriz geradora sob a forma padrão.*

Demonstração. Veja [7, Teorema 1.6.2]. □

1.2.3 Matriz de Verificação e Dual

Vimos na Secção 1.2.2 que todo código $\mathcal{C}$ sobre $\mathbb{F}^n$ pode ser visto como núcleo de uma transformação linear $\varphi : \mathbb{F}^n \to \mathbb{F}^{n-k}$. Em particular, existe uma matriz $H_{n-k\times n}$, da transformação φ, de modo que $c \in \mathcal{C}$ se, e somente se, $Hc^T = 0$. Tal matriz H é denominada *matriz de verificação* para $\mathcal{C}$. Veremos que o conceito de ortogonalidade está relacionado com o de matriz de verificação.

Comecemos com a seguinte definição:

Definição 1.2.15. *Sejam $u = (u_1, ..., u_n), v = (v_1, ..., v_n) \in \mathbb{F}^n$. Definimos o **produto interno** de u com v como sendo*

$$\langle u, v\rangle = \sum_{i=1}^{n} u_i v_i.$$

Definição 1.2.16. *Seja $\mathcal{C}$ um código sobre $\mathbb{F}^n$. Definimos o **ortogonal** (dual) de $\mathcal{C}$ por*

$$\mathcal{C}^{\perp} = \{x \in \mathbb{F}^n : \langle x, c\rangle = 0, \forall c \in \mathcal{C}\}.$$

Proposição 1.2.17. *Se $\mathcal{C}$ é um (n, k)-código linear com matriz geradora G, então $\mathcal{C}^{\perp}$ é um código sobre $\mathbb{F}^n$ e $c^{\perp} \in \mathcal{C}^{\perp}$ se, e somente se, $G(c^{\perp})^t = 0$.*

Demonstração. Veja [6, Seção 5.3, Lema 1]. □

Proposição 1.2.18. *Seja $\mathcal{C}$ um (n, k)-código linear. Suponha que $\mathcal{C}$ admita matriz geradora $G = (Id_k|A)$ sob a forma padrão. Então:*

1. $\dim(\mathcal{C}^{\perp}) = n - k$;
2. *$H = (-A^T|Id_{n-k})$ é uma matriz geradora de $\mathcal{C}^{\perp}$.*

Demonstração. Veja [6, Seção 5.3, Proposição 2]. □

Lema 1.2.19. *Sejam $\mathcal{C}$ um (n, k) código sobre $\mathbb{F}$ e G uma matriz geradora para $\mathcal{C}$. Então, uma matriz H de ordem $n - k \times n$ sobre $\mathbb{F}$ é uma matriz geradora de $\mathcal{C}^{\perp}$ se, e somente se, $GH^T = (0)_{k\times n-k}$*

Demonstração. Veja [6, Seção 5.3, Lema 3]. □

Corolário 1.2.20. *Seja $\mathcal{C}$ um código linear sobre $\mathbb{F}^n$, então $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.*

Corolário 1.2.21. *Seja $\mathcal{C}$ um código linear sobre $\mathbb{F}^n$ e H uma matriz geradora de $\mathcal{C}^\perp$. Então, dado $c \in \mathbb{F}^n$, temos $c \in \mathcal{C}$ se, e somente se, $Hc^T = 0$.*

Definição 1.2.22. *Seja $\mathcal{C}$ um (n,k)-código linear sobre $\mathbb{F}$. Dizemos que uma matriz H de ordem $n-k \times n$ sobre $\mathbb{F}$ é uma* ***matriz verificação*** *(ou teste de paridade), se H for uma matriz geradora de $\mathcal{C}^\perp$. Também, dado $v \in \mathbb{F}^n$ denominamos o vetor $Hv^T \in \mathbb{F}^{n-k}$ de* ***síndrome*** *de v e denotamos $syn(v) := Hv^T$.*

O próximo resultado relaciona códigos equivalentes e o conceito de ortogonalidade.

Teorema 1.2.23. *Sejam $\mathcal{C}$ e $\tilde{\mathcal{C}}$ códigos lineares equivalentes, então $\mathcal{C}^\perp$ e $\tilde{\mathcal{C}}^\perp$ também são equivalentes.*

Demonstração. Primeiramente, se σ é um automorfismo de permutação, então $\langle\ ,\ \rangle$ é invariante por σ, isto é, $\langle u, v\rangle = \langle \sigma(u), \sigma(v)\rangle$ para quaisquer $u, v \in \mathbb{F}^n$. Suponha que $\mathcal{C} \sim \tilde{\mathcal{C}}$, então existe uma permutação $\sigma \in S_n$ de modo que $\sigma(\mathcal{C}) = \tilde{\mathcal{C}}$. Mostremos que $\mathcal{C}^\perp \sim \tilde{\mathcal{C}}^\perp$. De fato, temos $u \in \sigma(\mathcal{C}^\perp)$ se, e somente se, $\sigma^{-1}(u) \in \mathcal{C}^\perp$ se, somente se, $\langle \sigma^{-1}(u), c\rangle = 0$ para cada $c \in \mathcal{C}$. Isto equivale a termos $\langle u, \sigma(c)\rangle = 0$ para cada $c \in \mathcal{C}$ se, e somente se, $u \in \sigma(\mathcal{C})^\perp$. Assim, $\sigma(\mathcal{C}^\perp) = \sigma(\mathcal{C})^\perp = \tilde{\mathcal{C}}^\perp$. Portanto, $\mathcal{C}^\perp \sim \tilde{\mathcal{C}}$.

□

1.2.4 Conjunto de Informações

Seja $\mathcal{C} \subset \mathbb{F}^n$ um código linear de dimensão k. Existe uma matriz geradora G de ordem $k \times n$ para o código $\mathcal{C}$. Assim, as k linhas de G são linearmente independentes, uma vez que essas determinam uma base para $\mathcal{C}$ como um $\mathbb{F}$ espaço vetorial. Em particular, existem k colunas linearmente independentes em G. Logo, podemos definir o seguinte:

Definição 1.2.24. *Sejam $\mathcal{C}$ um (n,k)-código linear sobre $\mathbb{F}$ e $G = (g_{ij})_{k\times n}$ uma matriz geradora para $\mathcal{C}$. Considere $\mathcal{I} \subset \{1, \ldots, n\}$ com $|\mathcal{I}| = k$ um conjunto que indexa k colunas de G. Dizemos que $\mathcal{I}$ é um* ***conjunto de informações*** *para $\mathcal{C}$ se as colunas de G indexadas por $\mathcal{I}$ são linearmente independentes. De outro modo, $\mathcal{I} = \{i_1, \ldots, i_k\}$ é um*

conjunto de informações se:

$$\{(g_{1i_j}, \ldots, g_{ki_j}) : 1 \leq j \leq k\} \subset \mathbb{F}^n$$

é linearmente independente. Quando $\mathcal{I}$ é um conjunto de informações para $\mathcal{C}$, chamamos, o conjunto complementar de $\mathcal{I}$, $\mathcal{I}^c = \{1, \ldots, n\} \backslash \mathcal{I}$ de ***conjunto de redundâncias*** *ou* ***conjunto de posições de verificação*** *para $\mathcal{C}$. Além disso, dado um vetor $v = (v_1, \ldots, v_n) \in \mathbb{F}^n$, denominamos de* ***símbolos de informações*** *aos elementos v_i com $i \in \mathcal{I}$ e chamamos* ***símbolos de redundância*** *aos elementos v_j com $j \in \mathcal{I}^c$.*

Exemplo 1.2.25. Considere o código linear $\mathcal{C}$ em $\mathbb{F}_2^5$ gerado pela matriz

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

na forma padrão $(Id_4|A)$. Temos $\{1, 2, 3, 4\}$ e $\{1, 3, 4, 5\}$ formam conjuntos de informações para o código gerado por G cujas respectivas redundâncias são $\{5, 6, 7)\}$ e $\{2, 6, 7\}$. Note que, o conjunto $\{1, 2, 4, 7\}$ não é um conjunto de informação, pois a coluna 7 é combinação linear das colunas $1, 2$ e 4.

Observação 1.2.26. Se G é uma matriz geradora que é apresentada sob a forma padrão $G = (I_k|A)$ para um código (n, k)-código linear $\mathcal{C}$, então $\{1, ..., k\}$ sempre é um conjunto de informações e, consequentemente, $\{k+1, ..., n\}$ é sempre um conjunto de redundâncias. Além disso, se $(x_1, ..., x_n)$ é uma palavra em $\mathcal{C}$, então sua decodificação é exatamente a restrição $(x_1, ..., x_k)$.

O próximo resultado nos permite generalizar o que ocorre no exemplo acima para uma matriz G geral, que não necessariamente está na forma padrão. Em outras palavras, nosso objetivo é decodificar uma palavra do código conhecendo apenas uma matriz G e um conjunto de informações $\mathcal{I}$ associado a G.

Proposição 1.2.27. *Sejam $\mathcal{C}$ um (n, k) código linear sobre $\mathbb{F}$, $G = (g_{ij})_{k \times n}$ uma matriz geradora para $\mathcal{C}$ e $\mathcal{I} = \{i_1 < ... < i_k\}$ um conjunto de informações com respeito a G. Então*

1. *Se G_I é a submatriz de G obtida pela justaposição das colunas de G indexadas por $\mathcal{I}$, então $(G_I)^{-1}G := D$ é uma matriz geradora para $\mathcal{C}$.*

2. *Se* $c = \lambda D$ *com* $\lambda = (\lambda_1, \ldots, \lambda_k) \in \mathbb{F}^k$ *e* $c_{\mathcal{I}} = (c_{i_1}, \ldots, c_{i_k})$ *é a restrição de* c *às posições* $\mathcal{I}$*, então* $c_I = \lambda$.

Isso significa que cada palavra em $c \in \mathcal{C}$ *fica completamente determinada por suas entradas em* $\mathcal{I}$ *e, além disso,* $c_{\mathcal{I}}$ *é exatamente a decodificação de* c.

Demonstração. Veja que $(G_{\mathcal{I}})^{-1}$ é uma matriz cujas linhas determinamr uma $\mathbb{F}$-base para $\mathbb{F}^k$. Isso ocorre, uma vez que as colunas de $G_{\mathcal{I}}$ são linearmente independentes. Logo, cada $\lambda \in \mathbb{F}^k$ é escrito de modo único como $\lambda = \lambda'(G_{\mathcal{I}})^{-1}$ para um conveniente $\lambda' \in \mathbb{F}^k$. Como todo $c \in \mathcal{C}$ é da forma $c = \lambda G$, temos $c = \lambda'(G_{\mathcal{I}})^{-1}G = \lambda' D$, ou seja, D é uma matriz geradora para $\mathcal{C}$. De outra maneira, se

$$\begin{array}{rccc|rccc} \varphi: & \mathbb{F}^k & \to & \mathbb{F}^k & \psi: & \mathbb{F}^k & \to & \mathbb{F}^n \\ & \lambda & \mapsto & \lambda(G_{\mathcal{I}})^{-1} & & \lambda(G_{\mathcal{I}})^{-1} & \mapsto & (\lambda G_{\mathcal{I}})^{-1}G \end{array},$$

então $\varphi \circ \psi$ é um monomorfismo linear cuja imagem é $\mathcal{C}$. Deste modo, o item 1 fica provado. Para ver o item 2, considere $D = (d_{ij})_{k\times n}$,

$$G_{\mathcal{I}} = (v_{i_1} \ldots v_{i_k}) \text{ com } v_{i_j} = \begin{pmatrix} g_{1i_j} \\ \vdots \\ g_{ki_j} \end{pmatrix} \; e \; (G_{\mathcal{I}})^{-1} = \begin{pmatrix} u_{i_1} \\ \vdots \\ u_{i_k} \end{pmatrix}, \text{ com } u_{i_j} = (b_{i_j 1}, \ldots, b_{i_j k})^T,$$

ou seja, os v_{i_j} denotam as colunas de $G_{\mathcal{I}}$ e os u_{i_j} denotam as linhas de $(G_{\mathcal{I}})^{-1}$. Assim, temos

$$u_{i_s} v_{i_j} = b_{i_j 1} g_{1i_j} + \ldots + b_{i_j k} g_{ki_j} = \begin{cases} 0, & s \neq j \\ 1, & s = j. \end{cases}$$

Como consequência, se $d_{i_j} = (d_{1i_j} \ldots d_{ki_j})^T$ é a i_j-ésima coluna de D, então:

$$d_{1i_j} = u_{i_1} v_{i_j}, \ldots, d_{ki_j} = u_{i_k} v_{i_j},$$

implicando

$$d_{i_j} = \underbrace{(0, \ldots, 1, \ldots, 0)}_{\text{na posição } ji_j}{}^T.$$

Assim, se $c = \lambda D = (\lambda_1, \ldots, \lambda_k)D$, então $c_{\mathcal{I}} = (c_{i_1}, \ldots, c_{i_k})$ com

$$c_{i_j} = \lambda_1 d_{1i_j} + \ldots + \lambda_k d_{ki_j}, = \lambda_j$$

para cada $j = 1, \ldots, k$. Portanto, $c_{\mathcal{I}} = \lambda$, como queríamos. □

Observação 1.2.28. Note, em particular, que se $\mathcal{I}$ é um conjunto de informações para um código $\mathcal{C} \subset \mathbb{F}^n$ e $(c_1, \ldots, c_n)$ é uma palavra código, então, para cada $j \in \{1, \ldots, n\}$, existem escalares $\{a_{ij}\}_{i \in \mathcal{I}}$, tais que $c_j = \sum_{i \in \mathcal{I}} a_{ij} c_i$. Com efeito, basta considerar d_j a j-ésima coluna da matriz D, como na Proposição 1.2.27, temos $c_j = c|_{\mathcal{I}} \cdot d_j$.

O seguinte resultado mostra que conjuntos de informações são invariantes por automorfismos de permutação.

Proposição 1.2.29. *Considere $\mathcal{C}$ e $\tilde{\mathcal{C}}$ códigos lineares equivalentes, sobre o automorfismo de permutação σ, então $\mathcal{I}$ é um conjunto de informações para $\mathcal{C}$ se, e somente se, $\sigma(\mathcal{I})$ é um conjunto de informações para $\tilde{\mathcal{C}}$.*

Demonstração. Suponha que G é uma matriz geradora de $\mathcal{C}$ e $\mathcal{I}$ é um conjunto de informações para $\mathcal{C}$. Então, a matriz G' obtida de G através da imagem de σ possui as colunas de G permutadas. Logo, se u_{j_i} denotam as colunas linearmente independentes de G, indexadas por $\mathcal{I}$, então as colunas $u_{j_{\sigma(i)}}$ continuam sendo linearmente independentes, ou seja, $\{\sigma(i) : i \in \mathcal{I}\} = \sigma(\mathcal{I})$ é um conjunto de informações para $\tilde{\mathcal{C}}$. Para a recíproca, basta aplicar o mesmo argumento para $\tilde{\mathcal{C}}$ usando o automorfismo de permutação σ^{-1}. □

Como corolário imediato, temos:

Corolário 1.2.30. *Considerando $\mathcal{C}$ e $\tilde{\mathcal{C}}$ são códigos lineares equivalentes sobre o automorfismo de permutação σ, então $\mathcal{H}$ é um conjunto posições de verificação para $\mathcal{C}$ se, e somente se, $\sigma(\mathcal{H})$ é um conjunto posições de verificação para $\tilde{\mathcal{C}}$.*

Os conjuntos de informações de um código $\mathcal{C}$ estão intimamente ligados aos conjuntos de posições de verificação para $\mathcal{C}^{\perp}$.

Proposição 1.2.31. *Seja $\mathcal{C}$ um código linear, então $\mathcal{I}$ é um conjunto de informações para $\mathcal{C}$ se, e somente se, $\mathcal{I}$ é um conjunto de posições de verificação para $\mathcal{C}^{\perp}$.*

Demonstração. Veja [7, Teorema 1.6.2]. □

1.2.5 Decodificação por Permutação

A decodificação refere-se ao processo de detecção e correção de erros em um determinado código. Nesta subseção, abordaremos o método de decodificação por permutação.

Esse método é aplicável quando um código possui um número suficiente de automorfismos para garantir a existência de um conjunto de automorfismos que satisfaça determinadas condições. A descrição completa desse método pode ser encontrada em trabalhos como de MacWilliams [11] e Huffman [7].

Considere $\mathcal{C}$ um código linear e suponha que um vetor $c \in \mathcal{C}$ foi recebido como r. Como vimos no Corolário 1.2.21, se H é uma matriz de verificação para $\mathcal{C}$, tem-se que $syn(r) = Hr^T \neq 0$ se $r \notin \mathcal{C}$. Inicialmente, define-se o **vetor erro** como sendo a diferença entre r e c, isto é, $e = r - c$. Ainda $\omega(e)$ é exatamente o número de erros que foram cometidos. Também,

$$syn(e) = syn(r - c) = H(r - c)^T = Hr^T - Hc^T = syn(r).$$

Logo, a palavra recebida e o vetor erro possuem mesma síndrome. Agora, suponhamos que tenhamos um conjunto de informações $\mathcal{I}$ para um (n, k)-código linear $\mathcal{C}$ e que conheçamos a capacidade κ de $\mathcal{C}$, o seguinte resultado nos fornece uma condição necessária e suficiente para que o vetor erro $r = c + e$ tenha as posições de informações $\mathcal{I}$ corretas.

Teorema 1.2.32. *Seja $\mathcal{C}$ um (n, k)-código linear com capacidade κ. Suponha que H seja uma matriz de verificação para $\mathcal{C}$ sob a forma padrão. Se $r = c + e$ com $c \in \mathcal{C}$ e $\omega(e) \leq \kappa$, então os símbolos de informações de r estão corretos se, e somente se, $\omega(syn(r)) \leq \kappa$.*

Demonstração. Sem perda de generalidade, podemos supor $\mathcal{C}$ possui matriz geradora $G = (I_k|A)$ sob a forma padrão. Deste modo $H = [-A^T|I_{n-k}]$ é uma matriz de verificação para $\mathcal{C}$ e as k primeiras posições formam um conjunto de informações. Se os símbolos de informações de r estão corretos, então

$$Hr^T = Hc^T + He^T = He^T = e^t,$$

pois as primeiras k coordenadas de e são nulas. Assim,

$$\omega(syn(r)) = \omega(Hr^T) = \omega(e^T) \leq \kappa.$$

Reciprocamente, suponha que os símbolos de informações de r estão incorretos. Se $e = (e_1, \ldots, e_n)$, tome $e' = (e_1, \ldots, e_k) \neq 0$ e $e'' = (e_{k+1}, \ldots, e_n)$. Usando que, $\omega(x + z) \geq$

$\omega(x) - \omega(z)$, obtemos:

$$\begin{aligned}\omega(Hr^T) = \omega(He^T) = \omega(-A^T e'^T + e''^T) &\geq \omega(-A^T e'^T - \omega(e''^T) \\ &= \omega(e_1 I_k) + \omega(e_1 A) - [\omega(e_1) + \omega(e_2)] \\ &= \omega(e_1 G) - \omega(e) \\ &\geq 2t + 1 - 1 = t + 1.\end{aligned}$$

□

Observação 1.2.33. Note que a hipótese no Teorema 1.2.32 sob a matriz H estar sob a forma padrão é razoável devido ao Teorema 1.2.14. Porém, tal suposição não é necessária, isto é, podemos supor H uma matriz qualquer e tomar um conjunto de informações arbitrário.

Definição 1.2.34. *Seja $\mathcal{C}$ um código linear sobre $\mathbb{F}$. Dada uma permutação $\sigma \in S_n$, podemos considerar o automorfismo linear:*

$$\begin{array}{rccc} \sigma : & \mathbb{F}^n & \to & \mathbb{F}^n \\ & (v_1, \ldots, v_n) & \mapsto & (v_{\sigma(1)}, \ldots, v_{\sigma(n)}) \end{array}$$

Definimos o ***grupo dos automorfismos de permutações*** *de $\mathcal{C}$, por*

$$\mathrm{PAut}(\mathcal{C}) = \{\sigma \in S_n \mid \sigma(\mathcal{C}) = \mathcal{C}\}.$$

Com cálculos rotineiros, vê-se que $\mathrm{PAut}(\mathcal{C})$ é, de fato, um grupo sob a operação de composição de funções. De maneira mais específica, $\mathrm{PAut}(\mathcal{C})$ constitui um subgrupo de S_n. Conforme mencionado anteriormente, o processo de decodificação por permutação envolve a utilização de um subconjunto apropriado de $\mathrm{PAut}(\mathcal{C})$, que mova os erros do vetor recebido r para posições fora das posições de informações. A definição a seguir formaliza o que significa ser um *conjunto apropriado* neste contexto.

Definição 1.2.35. *Seja $\mathcal{C}$ um código linear com capacidade κ. Diz-se que um subconjunto $X \subset \mathrm{PAut}(\mathcal{C})$ é um* ***PD-conjunto****, se para cada vetor erro possível, com peso menor ou igual a κ, existe ao menos um elemento de X que pode movê-lo para fora das posições de informações.*

Às vezes, observa-se que a decodificação por permutação não pode ser usada para corrigir a capacidade total de erro do código. A noção de decodificação por permutação parcial foi introduzida para corrigir um número menor de erros.

Definição 1.2.36. *Seja $\mathcal{C}$ um código linear com capacidade κ com conjunto de informações $\mathcal{I}$ e conjunto de posições de verificação $\mathcal{H}$. Para $s \leq \kappa$, um* ***s-PD-conjunto*** *é um subconjunto $X \subset \mathrm{PAut}(\mathcal{C})$ tal que cada conjunto de s posições de coordenadas é movido por pelo menos um elemento de X para $\mathcal{H}$ ou, equivalentemente, para fora de $\mathcal{I}$.*

Algoritmo de decodificação por permutação

Sejam $\mathcal{C}$ um (n, k) código linear com capacidade κ, H uma matriz de verificação para $\mathcal{C}$ sob a forma padrão e $X = \{\sigma_1, \ldots, \sigma_s\}$ um PD-conjunto. Suponha que uma palavra-código c tenha sido recebida como r e que no máximo κ erros ocorreram. A decodificação por permutação é realizada usando o seguinte algoritmo:

1. Para o vetor r recebido, calcule $\omega(H(\sigma_i(r))^T)$, para cada $i = 1, \ldots, s$, até que para algum i_0 tenhamos $\omega(H(\sigma_{i_0}(r))^T) \leq \kappa$.

2. Pelo Teorema 1.2.32, os símbolos de informações de

$$\sigma_{i_0}(r) = \sigma_{i_0}(c) + \sigma_{i_0}(e)$$

   estão corretos. Logo, nas posições de $\mathcal{I}$ os coeficientes de e é zero. Assim, nas posições de $\mathcal{I}$, $\sigma_{i_0}(r)$ contém exatamente os símbolos de informações de $c' = \sigma_{i_0}(c) \in \mathcal{C}$. Denote por $c'_{\mathcal{I}}$ esses símbolos de informações.

3. Construa a palavra $c' = c'_{\mathcal{I}} D$, em que D é a matriz obtida na Proposição 1.2.27.

4. Decodifique r como sendo $c = \sigma_{i_o}^{-1}(c')$.

O algoritmo é valido, uma vez que, para qualquer $\sigma \in S_n$, se $r = c + e$ com $c \in \mathcal{C}$, $\sigma(r) = \sigma(c) + \sigma(e)$ e, se $\sigma \in \mathrm{PAut}(\mathcal{C})$, então $\sigma(c) \in \mathcal{C}$.

Existem alguns problemas na decodificação por permutação. Primeiramente, o PD-conjunto relativo a um determinado conjunto de informações $\mathcal{I}$ pode ser excessivamente grande, o que pode tornar o algoritmo menos eficiente. Ou seja, quanto menor a quantidade de elementos em um PD-conjunto, menores são os custos computacionais.

O segundo problema está relacionado à obtenção de um PD-conjunto para um conjunto de informações fixo. Essa tarefa pode ser essencialmente complicada e, em alguns casos, pode até não ser possível. No Capítulo 3, construiremos um conjunto de informações para uma família de códigos, denotado por $\Gamma(\mathcal{C})$, e apresentaremos um PD-conjunto para este.

1.3 Códigos Cíclicos

Neste momento, direcionaremos nossa atenção para uma classe de códigos de extrema importância, denominada códigos cíclicos. Os códigos cíclicos foram estudados pela primeira vez por Prange em 1957 e originalmente foram introduzidos porque podiam ser eficientemente implementados. Atualmente esses códigos continuam despertando o interesse de matemáticos pois possuem uma estrutura algébrica muito rica. Mostraremos que esses códigos podem ser identificados como ideais de um certo anel, permitindo assim a utilização de outras ferramentas algébricas para o estudo de códigos.

1.3.1 Estrutura dos Códigos Cíclicos

A principal propriedade que caracteriza os códigos cíclicos é que eles são fechados para o deslocamento cíclico de suas palavras.

Definição 1.3.1. *Definimos o* ***deslocamento cíclico*** *sobre* $\mathbb{F}^n$*, como sendo a aplicação:*

$$\begin{array}{rccc} \pi: & \mathbb{F}^n & \to & \mathbb{F}^n \\ & (v_0, v_1, \ldots, v_{n-1}) & \mapsto & (v_{n-1}, v_0, \ldots, v_{n-2}) \end{array}.$$

Diz-se que um código linear $\mathcal{C} \subset \mathbb{F}^n$ *é* ***cíclico*** *se* $\mathcal{C}$ *é fechado por deslocamentos cíclicos, isto é,* $\pi(\mathcal{C}) = \mathcal{C}$*.*

Note que o deslocamento cíclico é um automorfismo linear sobre $\mathbb{F}^n$ e, além disso, se $\mathcal{C}$ é um código cíclico e τ é um n-ciclo em S_n, então $\tau(\mathcal{C}) = \mathcal{C}$. Ou seja, $\mathcal{C}$ é fechado por permutações cíclicas.

Para compreender melhor a estrutura algébrica por trás de códigos cíclicos usamos a seguinte representação polinomial de palavras-código: para cada palavras $c = (c_0, \ldots, c_{n-1})$ associamos de forma canônica o polinômio $c(x) = c_0 + c_1X + \ldots + c_{n-1}X^{n-1}$.

O seguinte teorema formaliza essa correspondência entre palavras-códigos e polinômios.

Teorema 1.3.2. *Considere o polinômio* $X^n - 1$ *sobre* $\mathbb{F}$ *e denote* $\mathcal{A}(n) := \dfrac{\mathbb{F}[X]}{[X^n - 1]}$*, temos:*

1. *Para cada* $f(X) \in \mathbb{F}[X]$*, existe* $r(X) \in \mathbb{F}$ *tal que,* $f(X) \equiv r(X) \pmod{X^n - 1}$ *com*

$r(X) = 0$ *ou* $\partial(r(X)) < n$. *Ou seja,*

$$\mathcal{A}(n) = \{f(X) \mid \partial(f(X) < n\}$$

2. $\mathcal{A}(n)$ *é um* $\mathbb{F}$*-espaço vetorial de dimensão finita* n *e uma base para* $\mathcal{A}(n)$ *é dada por* $\mathscr{B} = \{1, X, \ldots, X^{n-1}\}$;

3. *Existe uma correspondência linear bijetiva entre* $\mathbb{F}^n$ *e* $\mathcal{A}(n)$.

Demonstração. Veja [10, Teorema 7.2.1]. □

Um isomorfismo linear entre $\mathbb{F}^n$ e $\mathcal{A}(n)$ é dado explicitamente por:

$$\begin{array}{rccc} \mu: & \mathbb{F}^n & \to & \mathcal{A}(n) \\ & (c_0, c_1, \ldots, c_{n-1}) & \mapsto & c_0 + c_1X + \ldots + c_{n-1}X^{n-1} \end{array} \tag{1.2}$$

como pode ser verificado com alguns cálculos simples. A aplicação linear μ tem uma propriedade particularmente interessante, pois ela induz uma correspondência bijetora entre os códigos cíclicos de $\mathbb{F}^n$ e os ideais de $\mathcal{A}(n)$. Para provar isto, precisaremos do seguinte lema:

Lema 1.3.3. *Seja* S *um* $\mathbb{F}$*-subespaço vetorial de* $\mathcal{A}(n)$. *Então,* S *é um ideal de* $\mathcal{A}(n)$ *se, e somente se,* S *é fechado pela multiplicação por* X.

Demonstração. Se S é um ideal, então, pela própria definição de ideal, $Xs(X) \in S$ para qualquer que seja $s(X) \in S$. Reciprocamente, seja $a(X) \in S$. Como S é, em particular, um subespaço de A_n, temos que $ua(X) \in S$ para cada $u \in \mathbb{F}$. Como, por hipótese, $Xa(X) \in S$ então, por indução, $X^m a(X) \in S$ para cada $m \in \mathbb{N}$. Agora, seja $g(X) = b_0 + b_1X + \ldots + b_{n-1}X^{n-1} \in \mathcal{A}(n)$ tomado arbitrariamente. Veja que,

$$\begin{aligned} g(X)a(X) &= (b_0 + b_1X + \ldots + b_{n-1}X^{n-1})a(X) \\ &= b_0a(X) + b_1Xa(x) + \ldots + b_{n-1}X^{n-1}a(X) \in S. \end{aligned}$$

Portanto, S é um ideal de $\mathcal{A}(n)$. □

Teorema 1.3.4. *Um subespaço* $\mathcal{C}$ *de* $\mathbb{F}^n$ *é um código cíclico se, somente se,* $\mu(\mathcal{C})$ *é um ideal de* $\mathcal{A}(n)$.

Demonstração. Como μ é um isomorfismo de espaço vetoriais, segue-se que $\mu(\mathcal{C})$ é um subespaço vetorial de $\mathcal{A}(n)$. Assim, resta mostrar que, para $c(X) \in \mathcal{C}$ e $f(X) \in A_n$, tem-se $f(X)c(X) \in \mathcal{C}$. Ora, mas isso equivale a termos $Xc(X) \in \mathcal{C}$. Mas, pelo Lema 1.3.3, isso ocorre se, e somente se, $\mu(\mathcal{C})$ é um ideal de $\mathcal{A}(n)$. □

Como corolário imediato, temos:

Corolário 1.3.5. *Existe uma correspondência bijetiva entre os códigos cíclicos de $\mathbb{F}^n$ e os ideais de $\mathcal{A}(n)$*

Demonstração. A correspondência é dada explicitamente por:

$$\begin{array}{ccc} \{\mathcal{C} \subset \mathbb{F}^n \mid \mathcal{C} \text{ é um código cíclico}\} & \to & \{\text{ideais de } \mathcal{A}(n)\} \\ \mathcal{C} & \mapsto & \mu(\mathcal{C}) \\ \mu^{-1}(I) & \leftarrow\!\shortmid & I \end{array}$$

□

Devido à correspondência acima é comum pensar em códigos cíclicos simplesmente como ideais. Assim, daqui por diante, adotamos os termos *códigos cíclicos* e *ideais* como sinônimos.

1.3.2 Raízes de $X^n - 1$

Devido aos estudos feitos na subsecção anterior, é natural buscar entender a estrutura dos ideais de $\mathcal{A}(n)$ e para isso é essencial estudar a estrutura das raízes de $X^n - 1$.

Teorema 1.3.6. *Seja $\mathcal{C}$ um código cíclico de $\mathcal{A}(n)$, então:*

1. *Existe um polinômio mônico $g(X)$ de menor grau em $\mathcal{C}$ e $\mathcal{C} = [g(X)]$;*
2. *$g(X)$ é um divisor de $X^n - 1$;*

Demonstração. Veja [6, Secção 6.2, Proposição 1]. □

O polinômio $g(X)$, como na proposição anterior, é denominado **polinômio gerador** para o código cíclico $\mathcal{C}$. O próximo resultado relaciona o grau do polinômio gerador e a dimensão do código.

Teorema 1.3.7. *Seja $\mathcal{C}$ um código cíclico de $\mathcal{A}(n)$ com polinômio gerador $g(X)$, se $\partial(g(X)) = k$ então $dim(\mathcal{C}) = n - k$. Além disso, uma base para $\mathcal{C}$ é dada explicitamente por $\mathscr{B} = \{g(X), Xg(X), \ldots, X^k g(X)\}$. Ainda, se $g(X) = g_0 + g_1X + \ldots g_kX^k$ então a matriz*

$$G = \begin{pmatrix} g_0 & g_1 & \cdot & \cdot & \cdot & g_k & 0 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & g_0 & g_1 & \cdot & \cdot & \cdot & g_k & 0 & \cdot & \cdot & \cdot & 0 \\ \cdot & & & & & & & & & & & \cdot \\ \cdot & & & & & & & & & & & \cdot \\ \cdot & & & & & & & & & & & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot & g_0 & g_1 & \cdot & \cdot & \cdot & \cdot & g_k \end{pmatrix}$$

gera o código cíclico correspondente a $\mathcal{C}$ em $\mathbb{F}^n$.

Demonstração. Veja [7, Teorema 4.2.1]. □

Observação 1.3.8. É possível verificar que em todo código cíclico $\mathcal{C}$ de dimensão k, quaisquer k índices consecutivos determinam um conjunto de informações para $\mathcal{C}$. Com efeito, se G é a matriz gerado para $\mathcal{C}$ como no Teorema 1.3.7, temos $g_0 \neq 0$, pois $g(X)$ é um polinômio minimal. Assim as k primeiras colunas de G são linearmente independentes e, consequentemente, determinam um conjunto de informações para $\mathcal{C}$. Logo, o automorfismo $\sigma \in \mathrm{PAut}(\mathcal{C})$, definido por $\sigma(1, \ldots, n) = (n, 1, \ldots, n-1)$, age em G deslocando suas colunas em 1 posição. Assim, após a aplicação de σ obtemos outro conjunto de informações $2, \ldots, k+1$. Aplicando esse argumento sucessivas vezes, obtemos que quaisquer k coordenadas consecutivas determinam um conjunto de informações para $\mathcal{C}$.

Agora, voltaremos a estudar os códigos cíclicos a partir de suas raízes. Nesse contexto, é comum almejar que as raízes do polinômio gerador $g(X)$ sejam distintas em alguma extensão de $\mathbb{F} = \mathbb{F}_q$ que contenha as raízes de $g(X)$, ou ainda, como queremos estudar todos os ideais de $\mathcal{A}(n)$, uma extensão em que $X^n - 1$ possua raízes simples, pois, se isso ocorrer, podemos fazer o uso de toda a teoria desenvolvida nas Subseções 1.1.3 e 1.1.3. Adiantamos que isso ocorre se, e somente se, $\mathrm{mdc}(q, n) = 1$ como provaremos agora:

Lema 1.3.9. *O polinômio $X^n - 1$ possui todas as suas raízes simples em uma extensão de $\mathbb{F}_q \subset \mathbb{F}_{q^m}$ se, e somente se, $mdc(q, n) = 1$.*

Demonstração. Primeiramente, suponha que $mdc(n,q)=1$ e vejamos que $\mathbb{F}_q$ admite uma extensão em que X^n-1 se fatora em termos lineares. De fato, pela hipótese q é invertível módulo n, isto é, existe um menor inteiro positivo m tal que $q^m \equiv 1 \pmod{n}$ o que ocorre se, e somente se, $n \mid q^m-1$. Também, q^m-1 é a ordem do grupo cíclico $\mathbb{F}_{q^m}^*$. Assim, deve existir $\alpha \in \mathbb{F}_{q^m}^*$ com $\circ(\alpha)=n$. Deste modo, $\alpha^n=1$ e α é raiz de X^n-1. Ademais, as potências $1,\alpha,\ldots,\alpha^{n-1}$ são raízes de X^n-1 que são distintas. Logo,

$$X^n-1=(X-1)(X-\alpha)\cdot\ldots\cdot(X-\alpha^{n-1}).$$

Reciprocamente, suponha que $mdc(q,n)\neq 1$, então $p \mid n$ e podemos escrever $n=p^r n'$ com $mdc(n',p^r)=1$. Note que $X^n-1=X^{np^r}-1=(X^{n'}-1)^{p^r}$. Por outro lado, como $mdc(p,n')=1$, existe uma extensão de $\mathbb{F}_p$ de modo que $X^{n'}-1$ se decompõe em fatores lineares. Como $X^n-1=(X^{n'}-1)^{p^r}$ e $p^r \geq p$ segue X^n-1 tem raízes múltiplas. □

Definição 1.3.10. *O elemento α obtido no Lema 1.3.9 é denominado n-ésima* ***raiz primitiva da unidade****.*

Daqui por diante vamos supor sempre que $\mathbb{F}$ é um corpo de ordem q e n é um inteiro positivo relativamente primo com q e, portanto, X^n-1 possui suas raízes distintas em uma extensão $\mathbb{F}_{q^m}$ de $\mathbb{F}$.

Agora, considere $\gamma \in \mathbb{F}_{q^m}$ um elemento primitivo e seja $d=\dfrac{q^m-1}{n}$, então a ordem de $\alpha=\gamma^d$ é n, isto é, α é um n-ésima raiz primitiva da unidade. Deste modo, as raízes do polinômio $M_{\alpha^s}(X)$ são, pela Proposição 1.1.29, dadas por:

$$\{\gamma^{ds},\gamma^{dsq},\ldots,\gamma^{dsq^{r-1}}\}=\{\alpha^s,\alpha^{sq},\ldots,\alpha^{sq^{r-1}}\}$$

Em que, r é o menor inteiro positivo tal que $dsq^r \equiv ds \pmod{q^m-1}$, o que ocorre se, e somente se, $sq^r \equiv s(mod\ n)$, pois o grupo multiplicativo gerado por α tem ordem n e, consequentemente,

$$\gamma^{dsq^r}=\gamma \iff \alpha^{sq^r}=\alpha^s \iff \alpha^{sq^r-s}=1 \iff sq^r-s\equiv 0(mod\ n).$$

Assim, podemos generalizar o conceito de classes ciclotômicas como segue:

Definição 1.3.11. *Sejam q e n inteiros relativamente primos. Dado um inteiro s, definimos a q-classe ciclotômica de s módulo n, ou q-****órbita*** *de s, como sendo o conjunto:*

$$C_n(s) =: \{s,sq,\ldots,sq^{r-1}\}(mod\ n)$$

em que r é o menor inteiro positivo tal que $sq^r \equiv s(mod\ n)$.

Observação 1.3.12. De modo exatamente análogo ao que foi feito na Subsecção 1.1.3 pode-se provar que a relação em $\mathbb{Z}_n$, definida por:

$$a, b \in \mathbb{Z}_n, a \sim b \iff a \in C_n(b)$$

é uma relação de equivalência e, portanto, as q-classes ciclotômicas módulo n determinam uma partição de $\mathbb{Z}_n$.

Como decorrência da Proposição 1.1.29, temos:

Teorema 1.3.13. *Sejam n e q inteiros relativamente primos e m a ordem de q módulo n. Se $\alpha \in \mathbb{F}_{q^m}$ é uma n-ésima raiz primitiva da unidade, temos:*

(1) Para cada $0 \leq s < n$,

$$M_{\alpha^s}(X) = \prod_{i \in C_n(s)} (X - \alpha^i).$$

(2) Os conjugados de α^s são os elementos da forma α^i com $i \in C_n(s)$.

(3) Além disso,

$$X^n - 1 = \prod_s M_{\alpha^s},$$

em que s percorre um e só um representante de cada q-classe ciclotômica módulo n.

Proposição 1.3.14. *A cardinalidade de uma q-classe ciclotômica módulo n é um divisor da ordem de q módulo n.*

Demonstração. Sejam m a ordem de q módulo n e $t = |C_n(s)|$ para algum s tomado arbitrário. Considere α uma n-ésima raiz primitiva da unidade em $\mathbb{F}_{q^m}$. O polinômio M_{α^s} tem grau t. Assim, devido o Teorema 1.1.22, t é um divisor de m. □

1.3.3 Raízes de Códigos Cíclicos

Como vimos, dado um código cíclico $\mathcal{C}$ em $\mathcal{A}(n) = \mathbb{F}[X]/[X^n - 1]$, existe um único polinômio mônico $g(X)$ de menor grau em $\mathcal{C}$ que gera $\mathcal{C}$ e, além disso, $g(X)$ é um divisor de $X^n - 1$. Considere $g(X) = p_1^{r_1}(X) \cdot \ldots \cdot p_r^{r_t}(X)$ a decomposição de $g(X)$, sobre $\mathbb{F}$, como produto de polinômios irredutíveis. Devido à hipótese sobre n ser relativamente primo

com a ordem de $\mathbb{F}$, pelos Teoremas 1.1.22 e 1.3.13, $r_i = 1$ e $p_i(X) = M_{\alpha^{s_i}}(X)$, em que α é uma n-ésima raiz primitiva da unidade, visto que $g(X)$ é um divisor de $X^n - 1$. Assim,

$$g(X) = \prod_{i=1}^{t} M_{\alpha^{s_i}}(X) = \prod_{i=1}^{t} \left(\prod_{j \in C_n(s_i)} (X - \alpha^j) \right)$$

Veremos que as raízes α^{s_i} de $g(X)$ bem como as classes ciclotômicas $C_n(s_i)$ caracterizam completamente o código $\mathcal{C}$.

No que segue, fixamos α como sendo uma n-ésima raiz primitiva da unidade que existe em alguma extensão de $\mathbb{F}$. Para provar a caracterização citada anteriormente, precisaremos antes de algumas definições:

Definição 1.3.15. *Considere $\mathcal{C} \subset \mathcal{A}(n)$ um código cíclico com polinômio gerador:*

$$g(X) = \prod_{i=1}^{t} \left(\prod_{j \in C_n(s_i)} X - \alpha^j \right).$$

*O **conjunto definidor** de $\mathcal{C}$ é dado por:*

$$\mathcal{D}(\mathcal{C}) := \bigcup_{s_i} C_n(s_i) \subset \mathbb{Z}_n.$$

Além disso, dizemos que o conjunto $\{s_i : 1 \leq i \leq t\}$ é um conjunto completo de representantes de q-classes ciclotômicas para o código $\mathcal{C}$.

Lema 1.3.16. *Seja $\mathcal{C}$ um código cíclico de $\mathcal{A}(n)$ com conjunto definidor $\mathcal{D}(\mathcal{C})$, então um elemento $c(X) \in \mathcal{A}(n)$ pertence a $\mathcal{C}$ se, e somente se, $c(\alpha^i) = 0$ para cada $i \in \mathcal{D}(\mathcal{C})$.*

Demonstração. Seja $g(X)$ o polinômio geradora de $\mathcal{C}$. Daí, se $c(X) \in \mathcal{C}$ então existe $h(X) \in \mathbb{F}[X]$ tal que, $c(X) \equiv h(X)g(X) \pmod{X^n - 1}$. Como para cada $\alpha^i \in \mathcal{D}(\mathcal{C})$ tem-se $g(\alpha^i) = 0$ segue $c(\alpha^i) = 0$. Reciprocamente, se $c(\alpha^i) = 0$ para cada $i \in \mathcal{D}(\mathcal{C})$, então $(X - \alpha^i) \mid c(X)$ para cada $i \in \mathcal{D}(\mathcal{C})$ e, portanto, $g(X) \mid c(X)$ e temos o desejado. □

Definição 1.3.17. *Dado um código cíclico $\mathcal{C} \subset \mathcal{A}(n)$, definimos o **conjunto de raízes** de $\mathcal{C}$ como sendo $\mathcal{Z}(\mathcal{C}) = \{\zeta \in \mathbb{F}_{q^m} \mid f(\zeta) = 0, \forall f \in \mathcal{C}\}$.*

Observação 1.3.18. Note que, se $\mathcal{C} = [g(X)]$, então $\mathcal{Z}(\mathcal{C}) = \{\zeta \in \mathbb{F}_{q^m} \mid g(\zeta) = 0\}$. Além disso, como $g(X) \mid X^n - 1$, temos $\mathcal{Z}(\mathcal{C}) \subset \{1, \alpha, \ldots, \alpha^{n-1}\}$.

Definição 1.3.19. *Considere $\mathcal{U} \subset \mathbb{Z}_n$, definimos o **código cíclico gerado** por $\mathcal{U}$, como sendo:*

$$I(\mathcal{U}) = \{f(X) \in \mathcal{A}(n) : f(\alpha^i) = 0, \forall i \in \mathcal{U}\}.$$

Note que o conjunto $I(\mathcal{U})$ esta bem definido, isto é, se $f(X) \equiv g(X) \pmod{X^n - 1}$ então $f(\alpha^i) = 0$, com $i \in \mathcal{U}$, se, e somente se, $g(\alpha^i) = 0$. De fato, $f(X) - g(X) = h(X)(X^n - 1)$ com $h(X) \in \mathbb{F}[X]$ conveniente. Ainda, como α é uma raiz da unidade, segue que $f(\alpha^i) - g(\alpha^i) = (\alpha^i)^n - 1 = 0$, implicando $f(\alpha^i) = g(\alpha^i)$. Também, com cálculos simples, vê-se que $I(\mathcal{U})$ é um código cíclico.

Definição 1.3.20. *Seja $\mathcal{U} \subset \mathbb{Z}_n$, diz-se que $\mathcal{U}$ é **fechado** se $\mathcal{U}$ for reunião de q-órbitas, isto é, reunião de q-classes ciclotômicas.*

Lembremos que, dado $\zeta \in \mathbb{F}_{q^m}$, a definimos $\mathbb{F}_q$-classe de ζ definida como sendo $cl(\zeta) = \{\beta \in \mathbb{F}_{q^m} \mid M_\zeta(X) = M_\beta(X)\}$. Além disso, se $\gamma \in \mathbb{F}_{q^m}$ é um elemento primitivo e $\gamma^s = \zeta$, então $cl(\zeta) = \{\gamma^i \mid i \in C_n(s)\}$.

Definição 1.3.21. *Dizemos que um subconjunto $\mathcal{V}$ de $\mathcal{R} := \{1, \alpha, \ldots, \alpha^{n-1}\}$ é **fechado** se, $\mathcal{V}$ for reunião de $\mathbb{F}_q$-classes de conjugados.*

Lema 1.3.22. *Seja $\mathcal{C}$ um código linear sobre $\mathcal{A}(n)$, temos:*

1. *$\mathcal{Z}(\mathcal{C})) = \{\alpha^i \mid i \in \mathcal{D}(\mathcal{C})\}$;*
2. *$\mathcal{Z}(\mathcal{C})$ é um subconjunto fechado de $\mathcal{R}$;*

Demonstração.

1. Temos, pelo Lema 1.3.16, que $h(X) \in I(\mathcal{U}))$ se, e somente se, $h(\alpha^i) = 0$ para cada $i \in \mathcal{D}(I(\mathcal{U})))$ se, e somente se, $\alpha^i \in \mathcal{Z}(I(\mathcal{U}))$.
2. Segue de imediato pelo item (1), pois $\mathcal{D}(I(U)) = \bigcup_{s_i} C_n(s_i)$ é reunião de convenientes q-órbitas e, portanto, $\mathcal{Z}(I(\mathcal{U})) = \bigcup_{s_i} cl(\alpha^{s_i})$.

□

O seguinte teorema mostra que o conjunto de raízes de um código cíclico o caracteriza completamente.

Teorema 1.3.23. *A família $\mathscr{C}(\mathcal{A}(n))$ de todos os códigos cíclicos de $\mathcal{A}(n)$ está em correspondência biunívoca com a família $\mathscr{F}(\mathcal{R})$ de todos os subconjuntos fechados de $\mathcal{R}$. Mais explicitamente, a aplicação*

$$\begin{array}{rccc} \chi: & \mathscr{C}(A_n) & \to & \mathscr{F}(\mathcal{R}) \\ & \mathcal{C} & \mapsto & \mathcal{Z}(\mathcal{C}) \end{array}$$

é uma bijeção, com inversa

$$\begin{array}{rccc} \chi^{-1}: & \mathscr{F}(\mathcal{R}) & \to & \mathscr{C}(\mathcal{A}(n)) \\ & \mathcal{V} & \mapsto & I(\mathcal{V}) \end{array}$$

Demonstração. Primeiramente, pelo Lema 1.3.22, a aplicação χ está bem definida. Assim, basta provar que χ^{-1} é de fato a inversa de χ ou, de maneira equivale, provar que:

$$I(\mathcal{Z}(\mathcal{C})) = \mathcal{C} \text{ e } \mathcal{Z}(I(\mathcal{V})) = \mathcal{V}.$$

De fato, inicialmente vejamos que $I(\mathcal{Z}(\mathcal{C})) = \mathcal{C}$. É claro que $\mathcal{C} \subset I(\mathcal{Z}(\mathcal{C}))$, pois todo elemento de $\mathcal{C}$ se anula em todo elemento de $\mathcal{Z}(\mathcal{C})$. Para a outra inclusão, se $g(X)$ e $h(X)$ geram $\mathcal{C}$ e $I(\mathcal{Z}(\mathcal{C}))$, respectivamente, então $g(X) \mid h(X)$, pois todas as raízes de $g(X)$ devem ser raízes de $h(X)$. Portanto, $I(\mathcal{Z}(\mathcal{C})) \subset \mathcal{C}$.

Agora, vejamos que $\mathcal{Z}(I(\mathcal{V})) = \mathcal{V}$. Uma inclusão é imediata, uma vez que todo elemento de $f(X) \in I(\mathcal{V})$ se anula para cada $\zeta \in \mathcal{V}$ e, consequentemente, $\mathcal{V} \subset \mathcal{Z}(I(\mathcal{V}))$. Agora, escreva $\mathcal{V} = \bigcup cl(\alpha^s)$ para convenientes potências de α e considere $g(X) = \prod M_{\alpha^s}(X)$. Temos $g(X) \in I(\mathcal{V})$. Logo, se $\zeta \in \mathcal{Z}(I(\mathcal{V}))$, então $g(\zeta) = 0$ o que, por sua vez, resulta $M_{\alpha^s}(\zeta) = 0$, para algum s. Assim, $\zeta \in cl(\alpha) \subset \mathcal{V}$. Portanto, o resultado fica provado. □

Como consequência temos os seguintes:

Corolário 1.3.24. *Existe uma correspondência biunívoca entre a família $\mathscr{F}(\mathbb{Z}_n)$ dos subconjuntos fechados de $\mathbb{Z}_n$ e $\mathscr{F}(\mathcal{R})$.*

Demonstração. Como já tínhamos observado, $cl(\alpha^s) = \{\alpha^i \mid i \in C_n(s)\}$. Assim, basta definir:

$$\begin{array}{rccc} \chi': & \mathscr{F}(\mathbb{Z}_n) & \to & \mathscr{F}(\mathcal{R}) \\ & \bigcup C_n(s) & \mapsto & \bigcup cl(\alpha^s) \end{array}.$$

□

Corolário 1.3.25. *Existe uma correspondência biunívoca entre $\mathscr{C}(\mathcal{A}(n))$ e $\mathscr{F}(\mathbb{Z}_n)$.*

Demonstração. Basta combinar o Teorema 1.3.4 com o Corolário 1.3.24. Além disso, tal bijeção leva o código cíclico $\mathcal{C}$ em seu conjunto definidor $\mathcal{D}(\mathcal{C})$. Portanto, $\mathcal{D}(\mathcal{C})$ também caracteriza completamente $\mathcal{C}$. □

Capítulo 2

Códigos Abelianos

O foco principal deste capítulo reside no estudo dos códigos abelianos. Para alcançar esse objetivo, é necessário introduzir previamente o conceito de anel de grupo, uma tarefa que será feita na Secção 2.1. Nesta seção, não apenas formalizamos essa estrutura algébrica, mas também apresentamos propriedades e resultados fundamentais que pavimentam o caminho para a progressão subsequente do Capítulo 3.

Prosseguindo, na Secção 2.2, definimos o conceito de *código de grupo*, oferecendo uma visão sucinta para a compreensão inicial desse conceito.

Aprofundando-nos na matéria, na Secção 2.3, definimos os códigos abelianos, explorando a análise através de suas raízes de maneira similar aos códigos cíclicos. Além disso, generalizamos os conceitos de classe de conjugados e classes ciclotômicas, dois aspectos essenciais para compreender a estrutura desses códigos.

Finalizando este capítulo, na Secção 2.4, introduzimos o conceito de *conjunto de informação* para essa classe mais abrangente de códigos. Nesta seção, também apresentamos a construção de um conjunto, denotado por $\Gamma(\mathcal{C})$, a partir da estrutura das classes ciclotômicas de um código abeliano arbitrário, cuja validade como conjunto de posições de verificação será demonstrada no Capítulo 3. Tal construção foi feita por Bernal e Jacobo em [2], esta que é a principal referência deste texto. Também, em [2], prova-se que $\Gamma(\mathcal{C})$ é um conjunto de posições de verificação.

2.1 Anel de Grupo

Nessa secção introduziremos uma nova estrutura algébrica, os **anéis de grupos**. Veremos que existe uma identificação natural entre os códigos cíclicos e uma classe de anéis de grupos. Além disso, tal identificação induz uma generalização natural dos códigos cícli-

cos, os códigos abelianos, os quais estudaremos posteriormente. As principais referências para essa secção são [15] e [1].

Sejam R um anel e G um grupo. Considere o conjunto RG formado por todas as somas formais do tipo

$$\sum_{g\in G} r_g g,$$

com $r_g \in R$, $g \in G$ e $r_g \neq 0$ apenas para um número finito de elementos $g \in G$.

Dados dois elementos $x = \sum_{g\in G} r_g g, y = \sum_{g\in G} s_g g \in RG$, temos $x = y$ se, e somente se, $r_g = s_g$, para cada $g \in G$. Sobre RG, definimos duas operações, a adição definida por:

$$\left(\sum_{g\in G} r_g g\right) + \left(\sum_{g\in G} r_g g\right) := \sum_{g\in G} (r_g + s_g)g$$

e a multiplicação dada por:

$$\sum_{g\in G} r_g g \cdot \sum_{h\in G} s_h h := \sum_{g,h\in G} r_g s_h gh.$$

Essas operações munem RG de uma estrutura de anel, como é de simples verificação, o qual é denominado **anel de grupo** com coeficientes em R e índices em G. O **zero** de RG é o elemento $\sum r_g g$, com $r_g = 0$, para cada $g \in G$. Além disso, se R possui unidade, então a unidade de RG é $1_{RG} = \sum r_g g$ em que $r_{1_G} = 1_R$ e $r_g = 0$ se $g \neq 1_G$ é o elemento neutro de G.

Observação 2.1.1. Daqui por diante, sempre que dissermos que R é um anel significará que R é um anel com unidade. Também, restringiremos os nossos estudos sobre anéis de grupos RG com R e G finitos.

O anel de grupo RG pode ser considerado de maneira natural como R-módulo. Basta definir a multiplicação por escalar, dada por:

$$\begin{array}{rccc} \cdot : & R \times RG & \to & RG \\ & (\lambda, \sum_g r_g g) & \mapsto & \sum_g \lambda r_g g \end{array}$$

Definição 2.1.2. *Seja M um R-módulo. Diz-se que um subconjunto $\mathscr{B} = \{b_i \in M : i \in I\} \subset M$ é um **conjunto gerador** para M se, para todo $b \in M$, existirem $i_1, \ldots, i_n$ e $r_i, \ldots, r_n \in R$ tais que,*

$$b = \sum_{i=j}^{n} r_j b_{i_j}.$$

Dizemos que um conjunto $B \subset M$ é ***linearmente independente*** *se, para qualquer subconjunto finito $\{i_1, \ldots, i_n\} \subset M$ e elementos $r_i, \ldots, r_n \in R$, temos*

$$\sum_{j=1}^{n} r_j b_{i_j} = 0 \iff r_1 = \ldots = r_n = 0$$

Se um conjunto gerador $\mathscr{B} \subset G$ é linearmente independente, então dizemos que $\mathscr{B}$ é um ***base*** *e, nesse caso, dizemos que M é um R-módulo* ***livre****.*

A proposição aseguir nos fornece maneiras de mergulhar o grupo G e o anel R no anel de grupo RG, isto é, existem identificações $i : G \hookrightarrow RG$ e $j : R \hookrightarrow RG$.

Proposição 2.1.3. *Sejam G um grupo e R um anel, então:*

1. *A aplicação*

$$\begin{array}{rccc} i: & G & \to & RG \\ & x & \mapsto & \sum_g a_g g \end{array} \; ; \; a_g = \begin{cases} 1, & g = x \\ 0, & g \neq x \end{cases}$$

   é injetiva.

2. *A aplicação*

$$\begin{array}{rccc} \mu: & R & \to & RG \\ & r & \mapsto & \sum_g a_g g \end{array} \; ; \; a_g = \begin{cases} r, & g = 1_G \\ 0, & g \neq 1_g \end{cases}$$

   define um homomorfismo injetor de anéis.

Demonstração. Veja [15, Secção 3.2]. □

Feitas as identificações acima, podemos dizer que $R, G \subset RG$. Ainda, dado $g \in G$ identificamos g como $1_R g$ em RG e dado $r \in R$ identificamos r como sendo $r1_G$ em RG. Assim, RG é um R-módulo livre com base $\mathscr{B} = G$.

Definição 2.1.4. *Seja R um anel comutativo. Uma R-****álgebra*** *é um anel com unidade A que possui estrutura de R-módulo de modo que,*

$$\alpha(ab) = (\alpha a)b = a(\alpha b)$$

para quaisquer $\alpha \in R$ e $a, b \in A$.

Com alguns cálculos rotineiros, pode-se verificar que:

Proposição 2.1.5. *Se R é um anel comutativo, então RG é uma álgebra sobre R. Nesse caso, dizemos que o anel de grupo RG é uma* ***álgebra de grupo****.*

Proposição 2.1.6. *(Propriedade Universal) Sejam G um grupo, A, R anéis tais que, $R \subset A$. Suponha que existe uma aplicação $f : G \to A$ tal que,*

$$f(gh) = f(g)f(h), \forall g, h \in G.$$

Então existe um homomorfismo de anéis $f^* : RG \to A$, que é R-linear, e torna o seguinte diagrama comutativo:

$$\begin{array}{ccc} G & \xhookrightarrow{i} & RG \\ & \searrow^{f} & \downarrow{\scriptstyle f^*} \\ & & A \end{array}$$

Onde i é a identificação de G em RG. Além disso, se $R \subset Z(A)$, em que $Z(A)$ denota o ***centro*** *do anel A, então f^* é um homomorfismo de R-álgebras.*

Demonstração. Com efeito, basta definir f^* como sendo:

$$\begin{array}{rccc} f^* : & RG & \to & A \\ & \sum r_g g & \mapsto & \sum r_g f(g) \end{array} .$$

□

Quando G e H são grupos isomorfos, então RG e RH são R-módulos isomorfos como segue do seguinte resultado:

Corolário 2.1.7. *Seja $f : G \to H$ um homomorfismo de grupo. Então existe um único homomorfismo de anéis $f^* : RG \to RH$ tal que,*

$$f^*(g) = f(g), \forall g \in G.$$

Também, se R é comutativo, então f^* é um homomorfismo de R-álgebras e se, além disso, f é um epimorfismo (monomorfismo), então f^* também é um epimorfismo (monomorfismo).

Demonstração. Defina a aplicação

$$\begin{array}{rccc} \varphi : & G & \to & RH \\ & g & \mapsto & 1_R f(g) \end{array}$$

Note que,

$$\varphi(gh) = 1_R f(g) 1_R f(h) = 1_R f(g) f(h) = \varphi(g)\varphi(h).$$

Logo, pela propriedade universal de anéis de grupo, existe um homomorfismo $f^* : RG \to RH$ de modo que, $f^*(g) = \varphi(g) = 1_R f(g) = f(g)$ em RH. Agora, suponha que f é injetiva e vejamos que f^* também é. De fato, tome $x = \sum_g a_g g \in RG$ tal que

$$f^*(x) = \sum_g a_g f(g) = \sum_{h \in H} 0_R h.$$

Reescrevendo $f^*(x)$, obtemos

$$f^*(x) = \sum_{h \in H} a_h h \ ; \ a_h = \begin{cases} 0, h \notin Im(f) \\ a_g, h = f(g). \end{cases}$$

Note que o coeficiente a_h é bem definido, pois sendo f injetiva, dado $h \in Im(f)$, existe um único $g \in G$ tal que $f(g) = h$. Logo, pelo princípio de igualdade, deve valer que $a_h = 0$, para todo $h \in H$. Em particular, $a_g = 0$, para todo $g \in G$, donde $x = 0_{RG}$. Assim, $\ker(f^*) = \{0_{RG}\}$ e f^* é injetiva. Por fim, suponha f sobrejetiva e tome $y = \sum r_h h \in RH$. Então podemos escolher para cada $h \in H$ um elemento $g_h \in G$ tal que $f(h) = g_h$. Considere o elemento $x = \sum r_f(g) g \in RG$, em que convencionamos $r_{f(g)} = 0$ se $g \neq g_h$ para cada $h \in H$. Assim, omitindo os coeficientes nulos, podemos escrever $x = \sum r_{f(g)} g_h$

$$\begin{aligned} f^*(x) = f^*\left(\sum r_{f(g)} g_h\right) &= \sum f^*(r_{f(g)} g_h) \\ &= \sum r_{f(g)} f^*(g_h) \\ &= \sum r_h h \\ &= y, \end{aligned}$$

portanto, f^* é sobrejetiva o que termina a prova. □

2.2 Códigos de Grupo

O seguinte resultado mostra como relacionar os códigos cíclicos de $\mathcal{A}(n) = \mathbb{F}[X]/[X^n - 1]$ com os ideais em uma álgebra de grupo.

Teorema 2.2.1. *Considere $C_n = \{1, g, \ldots, g^{n-1}\}$ um grupo cíclico de ordem n gerado por g, a aplicação:*

$$\begin{array}{rccc} \varphi: & \mathcal{A}(n) & \to & \mathbb{F}C_n \\ & \displaystyle\sum_{i=0}^{n-1} a_i X^i & \mapsto & \displaystyle\sum_{i=0}^{n-1} a_i g^i \end{array}$$

é um isomorfismo de $\mathbb{F}$-álgebras. Além disso, se μ é o isomorfismo linear dado pelo Teorema 1.3.4, então $\mathcal{C} \subset \mathbb{F}_n$ é um código cíclico se, e somente se, $(\mu \circ \varphi)(\mathcal{C})$ é um ideal de $\mathbb{F}C_n$.

Demonstração. A aplicação φ é $\mathbb{F}$-linear, pois dado $\lambda \in \mathbb{F}$ qualquer, tem-se:

$$\varphi\left(\lambda \sum_{i=0}^{n-1} a_i X^i\right) = \varphi\left(\sum_{i=0}^{n-1} \lambda a_i X^i\right) = \sum_{i=0}^{n-1} \lambda a_i g^i = \lambda\left(\sum_{i=0}^{n-1} a_i g^i\right).$$

Também, como $\mathscr{B} = \{1, X, \ldots, X^{n-1}\}$ é base para $\mathcal{A}(n)$ temos φ injetiva. Assim, resta ver que φ é um homomorfismo de anéis. Para tanto, basta ver que φ é compatível com a operação de multiplicação. De fato, $X^i X^j = X^{i+j} = X^{r_{ij}}$ onde r_{ij} é o resto da divisão de $i+j$ por n. Do mesmo modo, devido à estrutura de grupo cíclico, $g^i g^j = g^{r_{ij}}$. Logo, se $f(X) = \sum a_i X^i$ e $g(X) = \sum b_i X^i$, temos

$$\begin{aligned} \varphi(f(X))\varphi(g(X)) &= \sum_{i=0}^{n-1} a_i g^i \sum_{i=0}^{n-1} b_i g^i \\ &= \sum_{k=0}^{n-1} c_k g^k \\ &= \varphi(f(X)g(X)). \end{aligned}$$

em que $c_k = \sum a_i b_j$, com $i + j \equiv k \pmod{n}$ e tomamos $1 \leq k \leq n-1$. □

O Teorema 2.2.1 nos permite ver todo código cíclico $\mathcal{C}$ em $\mathbb{F}^n$ como um ideal na álgebra $\mathbb{F}C_n$ e, nesse caso, dizemos que $\mathcal{C}$ é um C_n-código. Assim, podemos generalizar esse conceito de modo natural como segue:

Definição 2.2.2. *Sejam G um grupo de ordem n, $E = \{e_0, \ldots, e_{n-1}\}$ a base canônica dos $\mathbb{F}$-espaço vetorial $\mathbb{F}^n$ e $\mathcal{C}$ um código linear sobre o corpo $\mathbb{F}$. Diz-se que $\mathcal{C}$ é um G-**código** se existe uma bijeção $\varphi : E \to G$ de modo que a extensão linear de φ, $\overline{\varphi} : \mathbb{F}^n \to \mathbb{F}G$, é tal que $\overline{\varphi}(\mathcal{C})$ é um ideal de $\mathbb{F}G$.*

Quando $\mathcal{G}$ é uma família de grupos, como, por exemplo, os grupos abelianos, nilpotentes, solúveis e assim por diante, dizer que $\mathcal{C}$ é um $\mathcal{G}$-código, significa dizer que existe $G \in \mathcal{G}$ tal que $\mathcal{C}$ é G-código. Por exemplo, caso $\mathcal{G} = \{\text{grupos abelianos}\}$, dizemos que um $\mathcal{G}$-código é um *código abeliano*.

Vejamos um exemplo:

Exemplo 2.2.3. Como vimos anteriormente, todo código cíclico $\mathcal{C} \subset \mathbb{F}^n$ é um C_n-código. Mais diretamente, se $E = \{e_0, \ldots, e_{n-1}\}$ é a base canônica de $\mathbb{F}^n$ e g é o gerador de C_n, defina $\sigma : E \to C_n$, definida por $\sigma(e_i) = g^i$. Temos que σ se estende a um isomorfismo linear $\overline{\sigma} : \mathbb{F}^n \to \mathbb{F}C_n$ tal que $\overline{\sigma}(\mathcal{C})$ é um ideal de $\mathbb{F}C_n$. Porém, a recíproca não é verdadeira, isto é, nem todo C_n-código é um código cíclico. Como exemplo, Considere o código linear $\mathcal{C} = \{(a, a, b, b) : a, b \in \mathbb{F}\} \subset \mathbb{F}^4$. Note que $\mathcal{C}$ não é cíclico. De fato, considere π o deslocamento cíclico, temos que $(1, 1, 0, 0) \in \mathcal{C}$, porém $\pi(1, 1, 0, 0) = (0, 1, 1, 0) \notin \mathcal{C}$. No entanto, $\mathcal{C}$ é um C_4-código. De fato, considere $G = C_4 = \langle g \rangle$ e defina $f : E \to G$ em que $f(e_1) = 1_G, f(e_2) = g^2, f(e_3) = gf(e_4) = g^3$. Considere $\phi : \mathbb{F}^4 \to \mathbb{F}G$ a extensão de f. Afirmo que, $\phi(\mathcal{C})$ é um ideal de $\mathbb{F}G$. Com efeito, dado $c = (a, a, b, b) \in \mathcal{C}$, temos

$$\phi(c) = a1_G + ag^2 + bg + bg^3.$$

Agora, tome

$$r = r_{1_G}1_G + r_g g + r_{g^2}g^2 + r_{g^3}g^3 \in \mathbb{F}G$$

um elemento qualquer. Daí,

$$\begin{aligned} r\phi(c) &= (a1_G + ag^2 + bg + bg^3)(r_{1_G}1_G + r_g g + r_{g^2}g^2 + r_{g^3}g^3) \\ &= (r_{1_G}a + r_g b + r_{g^2}a + r_{g^3}b)1_G \\ &+ (r_{1_G}a + r_g b + r_{g^2}a + r_{g^3}b)g^2 \\ &+ r_{1_G}b + r_g a + r_{g^2}b + r_{g^3}a)g \\ &+ (r_{1_G}b + r_g a + r_{g^2}b + r_{g^3}a)g^3 \\ &= f((x_1, x_1, x_2, x_2)) \end{aligned}$$

Assim, $r\phi(c) \in \phi(\mathcal{C})$ e sendo c e r tomados quaisquer, segue que $\phi(\mathcal{C})$ é um ideal e, portanto, $\mathcal{C}$ é um G-código.

2.3 Códigos Abelianos

Nessa seção nos restringiremos aos códigos abelianos, esses que são o foco do nosso estudo.

Dado um grupo abeliano finito G, existem inteiros positivos $n_1, \ldots, n_\ell$, tais que $G \simeq \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_l}$, veja o Teorema 2.1 presente em [16]. Logo, devido ao Corolário 2.1.7, segue-se que $\mathbb{F}G \simeq \mathbb{F}(\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_l})$ como $\mathbb{F}$-álgebras. Assim, basta estudar os códigos abelianos de $\mathbb{F}(\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_l})$, ou seja, os ideais da álgebra $\mathbb{F}(\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_l})$. Tal como os códigos cíclicos, existe uma caracterização para os códigos abelianos em termos de suas raízes. Comecemos com o seguinte teorema:

Teorema 2.3.1. *Sejam $n_1, \ldots, n_\ell$ inteiros positivos e considere o seguinte quociente de anéis:*

$$\frac{\mathbb{F}[X_1, \ldots, X_\ell]}{[X_1^{n_1} - 1, \ldots, X_\ell^{n_\ell} - 1]} := \mathcal{A}(n_1, \ldots, n_\ell).$$

Então, $\mathcal{A}(n_1, \ldots, n_\ell)$ tem estrutura de $\mathbb{F}$-álgebra e, além disso, $\mathcal{A}(n_1, \ldots, n_\ell)$ e $\mathbb{F}(\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_l})$ são álgebras isomorfas.

Demonstração. Note que $\mathbb{F} \subset \mathcal{A}(n_1, \ldots, n_\ell)$. Inicialmente, mostraremos a existência de uma função satisfazendo as hipóteses da Proposição 2.1.6. De fato, denote $G = \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_l}$ e defina:

$$\begin{array}{rccc} f: & G & \to & \mathcal{A}(n_1, \ldots, n_\ell) \\ & (g_1^{j_1}, \ldots, g_\ell^{j_\ell}) & \mapsto & X_1^{j_1} \ldots X_\ell^{j_\ell} \end{array}$$

Provemos que f está bem definida. Para isso, tome $g = (g_1^{j_1}, \ldots, g_\ell^{j_\ell})$ e $g' = (g_1^{i_1}, \ldots, g_\ell^{i_\ell})$ tais que $g = g'$, isto é, $g_k^{j_k} = g_l^{i_\ell}$ para cada $k = 1, \ldots, \ell$ o que ocorre se, e somente se, $j_k \equiv i_\ell \pmod{n_k}$ implicando que $X_k^{j_k} = X_k^{i_k}$ e, deste modo, $f(g) = f(g')$. Agora, note que

$$\begin{aligned} f((g_1^{j_1}, \ldots, g_\ell^{j_\ell}) \cdot (g_1^{i_1}, \ldots, g_\ell^{i_\ell})) &= f(g_1^{j_1+i_1}, \ldots, g_\ell^{j_\ell+i_\ell}) \\ &= (X_1^{j_1+i_1} \ldots X_\ell^{j_\ell+i_\ell}) \\ &= (X_1^{j_1} \ldots X_\ell^{j_\ell})(X_1^{i_1} \ldots X_\ell^{i_\ell}) \\ &= f(g_1^{j_1}, \ldots, g_\ell^{j_\ell}) f(g_1^{i_1}, \ldots, g_\ell^{i_\ell}). \end{aligned}$$

Logo, pela Proposição 2.1.6, existe um homomorfismo de anéis $f^* : \mathbb{F}G \to \mathcal{A}(n_1, \ldots, n_\ell)$ que é $\mathbb{F}$-linear. Além disso, como $\mathscr{B} = \{X_1^{j_1} \ldots X_\ell^{j_\ell} \mid 0 \leq j_k < n_k; k = 1 \ldots, \ell\}$ é uma base para $\mathcal{A}(n_1, \ldots, n_\ell)$ e $\mathscr{B} \subset Im(f^*)$ segue que f^* é sobrejetiva. Finalmente, sendo $f^*|_G$ injetiva e G uma base para $\mathbb{F}G$ resulta que f^* é injetiva e, portanto, f^* é um isomorfismo de $\mathbb{F}$-álgebras. □

Lema 2.3.2. *Sejam $\mathbb{F} = \mathbb{F}_q$ e $f(X_1, \ldots, X_\ell)$ um polinômio com coeficientes em $\mathbb{F}$. Então*

$$f(X_1, \ldots, X_\ell)^{q^r} = f(X_1^{q^r}, \ldots, X_\ell^{q^r})$$

para qualquer que seja o inteiro positivo r.

Demonstração. O caso em que $r = 1$ segue-se similarmente a Proposição 1.1.2. Para ver o caso geral basta prosseguir por indução. □

Assim, se $\alpha = (\alpha_1, \ldots, \alpha_\ell)$ é uma raiz de um polinômio $f = f(X_1, \ldots, X_\ell)$ com coeficientes em $\mathbb{F}$, então $\alpha^q := (\alpha_1^q, \ldots, \alpha_\ell^q)$ também é raiz de f. Assim, podemos generalizar o conceito de $\mathbb{F}$-conjugado, como segue:

Definição 2.3.3. *Seja $\mathbb{F}_q \subset \mathbb{F}_{q^m}$ uma extensão de corpos com $\mathbb{K} = \mathbb{F}_{q^m}$. Dado $\beta = (\beta_1, \ldots, \beta_\ell) \in \mathbb{K}^\ell$, definimos a $\mathbb{F}_q$-**classe de conjugados** de β, como sendo o conjunto $cl(\beta) = \{\beta^{q^r} : r \in \mathbb{N}\}$*

Daqui por diante, assuma que $mdc(q, n) = 1$ com $n = n_1 \cdot \ldots \cdot n_\ell$. Assim, podemos considerar uma extensão de $\mathbb{F}_q$ que contenha uma n_i-ésima raiz primitiva da unidade, para cada $i = 1, \ldots, \ell$.

Definição 2.3.4. *Dado $i = 1, \ldots, \ell$ denotamos por α_i uma n_i-ésima raiz primitiva da unidade que existe em alguma extensão de $\mathbb{F}_q$. Também, consideramos,*

$$\mathcal{R} = \{\alpha^j := (\alpha_1^{j_1}, \ldots \alpha_\ell^{j_\ell}) \mid j = (j_1, \ldots, j_\ell) \in \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell}\},$$

isto é, $\mathcal{R}$ é o conjunto de todas as ℓ-uplas ordenadas cuja i-ésima coordenada é uma n_i-ésima raiz da unidade.

Lema 2.3.5. *Sejam $\mathbb{F}$ um corpo finito e $\beta \in \mathbb{F}$ uma n-ésima raiz primitiva da unidade. Seja r o menor inteiro positivo tal que, $\beta^{iq^r} = \beta^i$, isto é, $r = |C_n(i)|$, então $\beta^{iq^s} = \beta^i$ se, e somente se, $r \mid s$. Como consequência disso, temos $iq^s \equiv i (mod\ n)$ se, e somente se $r \mid s$.*

Demonstração. Primeiramente, provaremos que $\beta^{iq^{rk}} = \beta^i$ para cada $k \in \mathbb{N}$ o que será feito por indução sobre $k \geq 0$. Para $k = 0$ e $k = 1$ nada temos o que provar. Suponha que a hipótese seja verdadeira para $k \geq 1$ e vejamos que também é verdadeira para $k+1$. De fato,

$$\beta^{iq^{r(k+1)}} = \beta^{iq^{rk+r}} = \beta^{iq^{rk}.q^r} = (\beta^{iq^{rk}})^{q^r} = (\beta^i)^{q^r} = \beta^i.$$

Reciprocamente, dado um inteiro s, escreva $s = rk + t$ com $0 \leq t < r$, então:

$$\beta^{iq^s} = \beta^{iq^{rk+t}} = \beta^{iq^t}$$

e sendo $t < r$ temos que $\beta^{iq^t} = \beta^i$ se, e somente se, $t = 0$ e, portanto, r deve dividir s o que conclui a prova. □

O próximo resultado nos fornece a cardinalidade de uma $\mathbb{F}_q$-classe de um elemento $\alpha \in \mathcal{R}$.

Proposição 2.3.6. *Tome $\alpha^i = (\alpha_1^{i_1}, \ldots, \alpha_\ell^{i_\ell}) \in \mathcal{R}$, denote por $r_j = |C_{n_j}(i_j)|$ para cada $j = 1, \ldots, \ell$ e por $r = mmc(r_1, \ldots, r_\ell)$, então $|cl(\alpha^i)| = r$ e r é o menor inteiro positivo tal que $\alpha^{iq^r} = \alpha^i$, isto é, r é o menor inteiro positivo satisfazendo $i_k q^r \equiv i_k \pmod{n_k}$, para cada $k = 1, \ldots, \ell$.*

Demonstração. Como $r_i \mid r$ para cada $i = 1, \ldots, \ell$, do Lema 2.3.5, temos $\alpha^{iq^r} = \alpha^i$. Assim, se provarmos que os elementos $\alpha^i, \alpha^{iq^2}, \ldots, \alpha^{iq^{r-1}}$ são dois a dois distintos, teremos que $|cl(\alpha^i)| = r$. Com efeito, suponha que isto não a, ou seja, que exista $0 \leq s < t < r$, tais que $\alpha^{iq^s} = \alpha^{iq^t}$. Então $\alpha_j^{i_j q^s} = \alpha_j^{i_j q^t}$, para cada $j = 1, \ldots, \ell$. Logo, $\alpha_j^{i_j q^s - i_j q^r} = 1$ implicando $n \mid i_j q^s - i_j q^r$ ou, equivalentemente, $iq^t \equiv iq^s (mod\ n_j)$ se, e somente se, $iq^{t-s} \equiv i (mod\ n_j)$ e, consequentemente,$r_j \mid t - s, \forall j = 1, \ldots, \ell$. Daí, $r \mid t - s$, o que é uma contradição, pois $0 < t - s < t < r$. Portanto, $|cl(\alpha^i)| = r$. □

Também, podemos generalizar o conceito de classe ciclotômica para uma ℓ-upla de inteiros $(j_1, \ldots, j_\ell) \in \mathbb{Z}_{n_1} \times \ldots \mathbb{Z}_{n_\ell}$.

Definição 2.3.7. *Dado $j = (j_1, \ldots, j_\ell) \in \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell}$ definimos a q-classe ciclotômica de j módulo $(n_1, \ldots, n_\ell)$ ou, simplesmente, q-**órbita** de j, como sendo o conjunto*

$$\mathcal{O}(j) = \{(j_1 q^t, \ldots, j_\ell q^t) \in \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell} \mid t \in \mathbb{N}\}.$$

Tal como as classes ciclotômicas, as q-órbitas determinam uma partição de $G := \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell}$.

Proposição 2.3.8. *A relação sobre G, definida por:*

$$i \sim j \iff \exists t \in \mathbb{N} : j = iq^t$$

é uma relação de equivalência. Em que denotamos $i = (i_1, \ldots, i_\ell)$, $j = (j_1, \ldots, j_\ell)$ e $iq^t = (qi_1, \ldots, qi_\ell)$.

Demonstração. A propriedade reflexiva é trivialmente satisfeita, uma vez que $i = iq^0$ para qualquer que seja $i \in G$. Também $\sim$ é transitiva, pois se $i \sim j$ e $j \sim k$, existem $t_1, t_2 \in \mathbb{N}$, tais que $j = iq^{t_1}$ e $k = jq^{t_2}$. Logo, $k = iq^{t_1+t_2}$ e $i \sim k$. Finalmente, para ver que $\sim$ é simétrica, suponha que $i \sim j$, com $i = (i_1, \ldots, i_\ell)$ e $j = (j_1, \ldots, j_\ell)$, então existe $t \in \mathbb{N}$ de modo que $j_s \equiv i_s \pmod{n_s}$ para cada $s = 1, \ldots, \ell$. Como $mdc(q, n_1 \ldots n_\ell) = 1$, existe $t' \in \mathbb{N}$ satisfazendo $q^t q^{t'} \equiv 1 \pmod{n_1 \ldots n_\ell}$, em particular, $q^t q^{t'} \equiv 1 \pmod{n_s}$ para cada $s = 1, \ldots, \ell$. Assim, $j_s q^{t'} \equiv i_s \pmod{n_s}$ e, portanto, $i = jq^{t'}$ e temos a propriedade simétrica. □

Proposição 2.3.9. *Dados $\alpha^i \in \mathcal{R}$, temos $|cl(\alpha^i)| = |\mathcal{O}(i)|$. Além disso, $\alpha^j \in cl(\alpha^i)$ se, e somente se, $j \in \mathcal{O}(i)$.*

Demonstração. De fato, basta notar que a aplicação

$$\begin{array}{rccc} g: & cl(\alpha^i) & \to & \mathcal{O}(i) \\ & \alpha^{iq^t} & \mapsto & (i_1 q^t, ..., i_\ell q^t) \end{array} .$$

é uma bijeção. Além disso, se $j = (j_1, \ldots, j_\ell)$ e $i = (i_1, \ldots, i_\ell)$, tem-se:

$$\begin{aligned} \alpha^j \in cl(\alpha^i) &\iff \exists t \in \mathbb{N} : \alpha^j = \alpha^{iq^t} \\ &\iff \alpha_k^{j_k} = \alpha_k^{i_k q^t}, \forall k = 1, \ldots \ell \\ &\iff j_k \equiv i_k q^t (\quad (\text{mod } n_k), \forall k = 1, \ldots \ell \\ &\iff j \in \mathcal{O}(i). \end{aligned}$$

□

Pelo Teorema de Correspondência,

$$\mathcal{C} = \frac{C}{[X_1^{n_1-1}, \ldots, X_\ell^{n_\ell}]}$$

em que C é um ideal de $\mathbb{F}[X_1, \ldots, X_\ell]$ que contém $X_1^{n_1-1}, \ldots, X_\ell^{n_\ell}$ o qual ainda denotaremos por $\mathcal{C}$. Assim, podemos definir o conjunto de raízes e o conjunto definidor para um código abeliano $\mathcal{C} \leq \mathcal{A}(n_1, \ldots, n_\ell)$ como segue:

Definição 2.3.10. *Seja $\mathcal{C}$ um código abeliano em $\mathcal{A}(n_1, \ldots, n_\ell)$. Definimos* ***conjunto de raízes*** *de $\mathcal{C}$ como sendo $\mathcal{Z}(\mathcal{C}) = \{\beta = (\beta_1, \ldots, \beta_\ell) \in \mathbb{K}^\ell \mid f(\beta) = 0, \forall f \in \mathcal{C}\}$ em que avaliamos f como um polinômio em $\mathbb{F}[X_1, \ldots, X_\ell]$.*

Como $\mathcal{C}$ contém $X_i^{n_i} - 1$ para cada $i = 1, \ldots, \ell$ segue que $\mathcal{Z}(\mathcal{C}) \subset \mathcal{R}$. Assim, podemos escrever $\mathcal{Z}(\mathcal{C}) = \{\alpha^j = (\alpha_1^{j_1}, \ldots, \alpha_\ell^{j_\ell}) \in \mathcal{R} \mid f(\alpha^j) = 0, \forall f \in \mathcal{C}\}$.

Definição 2.3.11. *Dado um código abeliano $\mathcal{C}$ em $\mathcal{A}(n_1, \ldots, n_\ell)$. O* ***conjunto definidor*** *de $\mathcal{C}$ é $\mathcal{D}(\mathcal{C}) = \{j = (j_1, \ldots, j_\ell) \in \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell} \mid \alpha^j \in \mathcal{Z}(\mathcal{C})\}$.*

Observação 2.3.12. Se $\mathcal{C}$ um código abeliano em $\mathcal{A}(n_1, \ldots, n_\ell)$, temos $\mathcal{Z}(\mathcal{C}) = \{\alpha^j \mid j \in \mathcal{D}(\mathcal{C})\}$.

Definição 2.3.13. *Considere $\mathcal{U} \subset \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell}$, definimos o* ***código gerado*** *por $\mathcal{U}$, como sendo:*

$$I(\mathcal{U}) = \{f(X) \in \mathcal{A}(n_1, \ldots, n_\ell) : f(\alpha^i) = 0, \forall i \in \mathcal{U}\}.$$

Definição 2.3.14. *Dizemos que $\mathcal{U} \subset \mathcal{R}$ é fechado se $\mathcal{U}$ for reunião de $\mathbb{F}_q$-classes. Analogamente, diz-se que $\mathcal{V} \subset \mathbb{Z}_{n_1} \times \ldots \mathbb{Z}_{n_\ell}$ é fechado se $\mathcal{V}$ for reunião de q-órbitas. Além disso, denotamos por $\mathcal{F}(\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell})$ e $\mathcal{F}(\mathcal{R})$ as famílias de todos os fechados de $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell}$ e $\mathcal{R}$, respectivamente.*

Observação 2.3.15. Note que, para todo código abeliano $\mathcal{C} \leq \mathcal{A}(n_1, \ldots, n_\ell)$, $\mathcal{D}(\mathcal{C})$ e $\mathcal{Z}(\mathcal{C})$ são subconjuntos fechados.

O seguinte teorema fornece uma caracterização dos códigos abelianos de $\mathcal{A}(n_1, \ldots, n_\ell)$. A demonstração desse resultado é abordada por meio de duas metodologias distintas: a primeira se utiliza da Teoria de Caracteres em anéis de grupo, enquanto a segunda se apoia na Teoria de Bases de Gröbner. Dada a complexidade e extensão dessas teorias, que extrapolam o escopo desta pesquisa, optou-se por omitir as demonstrações neste contexto. Uma prova encontra-se em [5, Proposição 2.12].

Teorema 2.3.16. *Existe uma correspondência bijetiva entre os subconjuntos fechados de* $\mathcal{R}$ *e os códigos de* $\mathcal{A}(n_1, \ldots, n_\ell)$ *dada por:*

$$\begin{array}{rccc} \chi: & \mathscr{C}(\mathcal{A}(n_1, \ldots, n_\ell)) & \to & \mathcal{F}(\mathcal{R}) \\ & \mathcal{C} & \mapsto & \mathcal{Z}(\mathcal{C}) \end{array}$$

com inversa

$$\begin{array}{rccc} \chi^{-1}: & \mathcal{F}(\mathcal{R}) & \to & \mathcal{I}(\mathcal{A}(n_1, \ldots, n_\ell)) \ . \\ & \mathcal{V} & \mapsto & I(\mathcal{V}) \end{array}$$

Em particular, existe uma bijeção entre $\mathcal{F}(\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell})$ *e* $\mathscr{C}(\mathcal{A}(n_1, \ldots, n_\ell))$.

Com isso em mente, um código $\mathcal{C} \leq \mathcal{A}(n_1, \ldots, n_\ell)$ fica completamente determinado por suas raízes, e temos $\mathcal{C} = I(\mathcal{Z}(\mathcal{C}))$. Ainda, como $\mathcal{Z}(\mathcal{C}) = \{\alpha^j : j \in \mathcal{D}(\mathcal{C})\}$ segue que $\mathcal{C}$ também fica completamente determinado por seu conjunto definidor.

2.4 Conjunto de informações

Nessa secção construiremos um conjunto $\Gamma(\mathcal{C}) \subset \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell}$, com respeito a um código abeliano $\mathcal{C}$ em $\mathcal{A}(n_1, \ldots, n_\ell)$, e mostraremos, no Capítulo 3, que este é um conjunto posições de verificação para $\mathcal{C}$ e, como consequência, teremos $\Gamma(\mathcal{C})^c$ um conjunto de informações para $\mathcal{C}$.

Dado um código abeliano $\mathcal{C}$ em $\mathcal{A}(n_1, \ldots, n_\ell)$. Uma **palavra** em $\mathcal{C}$ é um polinômio $c = c(X_1, \ldots, X_\ell) \in \mathcal{C}$. Ainda, sendo

$$\mathscr{B} = \{X_1^{j_1} \ldots X_\ell^{j_\ell} \mid (j_1, \ldots, j_\ell) \in \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell}\}$$

uma base para $\mathbb{F}$-álgebra $\mathcal{A}(n_1, \ldots, n_\ell)$, podemos escrever c como sendo

$$c = \sum_{(j_1, \ldots, j_\ell)} \lambda_{(j_1, \ldots, j_\ell)} X_1^{j_1} \ldots X_\ell^{\ell}$$

para convenientes $\lambda_{(j_1, \ldots, j_\ell)} \in \mathbb{F}$.

Como vimos na Secção 1.2 um conjunto de informações para um (n, k)-código linear $\mathcal{C}$ é um conjunto de k índices de colunas linearmente independentes de uma matriz gerado para o código $\mathcal{C}$. Veja a Definição 1.2.24 para mais detalhes. Porém, sobre o anel polinomial de várias variáveis, não dispomos de uma forma padrão para a matriz geradora do código. Assim, nesse contexto, a definição de conjunto de informações é a que segue:

Definição 2.4.1. *Seja $\mathcal{C}$ um código abeliano em $\mathcal{A}(n_1, \ldots, n_\ell)$ de dimensão k. Diz-se que um subconjunto $\mathcal{I} \subset \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell}$ com $|\mathcal{I}| = k$ é um* ***conjunto de informações*** *para $\mathcal{C}$ se, dada qualquer palavra $c = \sum_{j \in \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell}} c_j X^j \in \mathcal{C}$, existem escalares $\{\lambda_{ij}\}_{i \in \mathcal{I}} \subset \mathbb{F}$, tais que $c_j = \sum_{i \in \mathcal{I}} \lambda_{ij} c_i$. Além disso, se $c \neq 0$ então tais escalares são unicamente determinados. Também, se $\mathcal{I}$ é um conjunto de informações, dizemos que $\mathcal{I}^c = \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell} \backslash \mathcal{I}$ é um* ***conjunto de posições de verificação*** *para $\mathcal{C}$.*

Dado um elemento $c = \sum \lambda_j X^j \in \mathcal{A}(n_1, \ldots, n_\ell)$, podemos definir o vetor $c' = (c_j)_{j \in G} \in \mathbb{F}^n$ em que $G = \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell}$. Também, dados $\mathcal{C}$ é um código sobre $\mathcal{A}(n_1, \ldots, n_\ell)$, $c \in \mathcal{C}$ e $\mathcal{I}$ um conjunto de informações para $\mathcal{C}$, denotamos por $c_\mathcal{I}$ o vetor $c_\mathcal{I} := (c_j)_{j \in \mathcal{I}} \in \mathbb{F}^{|\mathcal{I}|}$.

Como vimos na Proposição 1.2.27 , dados um código linear $\mathcal{C} \subset \mathbb{F}^n$ e $\mathcal{I}$ um conjunto de informações para $\mathcal{C}$, como na Definição 1.2.24, as palavras em $\mathcal{C}$ ficam unicamente determinadas por suas posições em $\mathcal{I}$, isto é, se duas palavras códigos coincidem nas posições $\mathcal{I}$, então elas devem coincidir nas demais posições. O seguinte resultado, mostra que isso também é verdade para um conjunto de informações $\mathcal{I}$ de um código abeliano arbitrário.

Lema 2.4.2. *Seja $\mathcal{I}$ um conjunto de informações para um código abeliano $\mathcal{C}$ em $\mathcal{A}(n_1, \ldots, n_\ell)$. Então, cada palavra $c \in \mathcal{C}$ fica unicamente determinada por seus símbolos nas posições em $\mathcal{I}$. Além disso, $\mathcal{C} \simeq \mathbb{F}^{|\mathcal{I}|}$ como $\mathbb{F}$-espaços vetoriais.*

Demonstração. De fato, tome c, d palavras em $\mathcal{C}$, tais que $c_\mathcal{I} = d_\mathcal{I}$. Considere $e = c - d$. Pela definição de conjunto de informações, para cada $j \in \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell}$, existem escalares $\{\lambda_{ij}\}_{i \in \mathcal{I}} \subset \mathbb{F}$, tais que:

$$e_j = \sum_{i \in \mathcal{I}} \lambda_{ij} e_i = \sum_{i \in \mathcal{I}} \lambda_{ij} (c_i - d_i) = \sum_{i \in \mathcal{I}} \lambda_{ij} 0 = 0 \in \mathbb{F},$$

donde $e_j = 0$. Da arbitrariedade de j, temos $e = 0$ e, portanto, $c = d$. Agora, considere a aplicação

$$\begin{array}{rccc} f: & \mathcal{C} & \to & \mathbb{F}^{|\mathcal{I}|} \\ & c & \mapsto & c_\mathcal{I} \end{array}.$$

Pelo que acabamos de provar, a aplicação f está bem definida e injetiva. Além disso, com cálculos simples é possível ver que f é uma transformação linear. Logo, $f(\mathcal{C}) \subset \mathbb{F}^{|\mathcal{I}|}$ é um subespaço de dimensão $|\mathcal{I}| = dim(\mathcal{C})$ e, portanto, $\mathcal{C} \simeq \mathbb{F}^{|\mathcal{I}|}$ como $\mathbb{F}$-espaços vetoriais. □

Antes de iniciar a construção do conjunto $\Gamma(\mathcal{C})$, é necessário estabelecer de forma clara e precisa alguns parâmetros auxiliares fundamentais para sua construção. Além disso, apresentaremos a demonstração de algumas propriedades inerentes a tais parâmetros.

Definição 2.4.3. *Seja $\mathcal{C} \subset \mathcal{A}(n_1, \ldots, n_\ell)$ um código abeliano. Dado um elemento $e = (e_1, \ldots, e_\ell)$ pertencente ao conjunto definidor $\mathcal{D}(\mathcal{C})$ e $1 \leq j \leq \ell$, definimos a* ***projeção das primeiras j coordenadas*** *pela aplicação*

$$\begin{array}{rccc} \pi_j : & \mathcal{D}(\mathcal{C}) & \to & \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_j} \\ & e & \mapsto & \pi_j(e) = (e_1, \ldots, e_j) \end{array} .$$

Denotaremos a imagem de $\mathcal{D}(\mathcal{C})$ através de π_j por $\mathcal{D}_j(\mathcal{C})$ também, por simplicidade, escreveremos que $e \in \mathcal{D}_j(\mathcal{C})$ em vez de $(e_1, \ldots, e_j) \in \mathcal{D}_j(\mathcal{C})$.

Definição 2.4.4. *Dado $n \in \mathbb{N}$ e $q = p^k$, com p primo, e $p \nmid n$, definimos para $\gamma, i \in \mathbb{Z}$ fixados a q^γ-classe ciclotômica de i módulo n como sendo o conjunto:*

$$C_{(q^\gamma, n)}(i) = \{iq^{\gamma j} : j \in \mathbb{N}\} \subset C_n(i).$$

Se $s = |C_{(q^\gamma, n)}(i)|$ então s é o menor inteiro positivo tal que $iq^{\gamma s} \equiv i \pmod{n}$. Em particular, devido ao Lema 2.3.5, $|C_n(i)|$ é um divisor de s.

A seguir, definimos parâmetros $\gamma_i(-)$ e $m(-)$ que dependem de um elemento $e \in \mathcal{D}_j(\mathcal{C})$. Tais parâmetros são números naturais construídos recursivamente.

Definição 2.4.5. *Estabelecemos uma ordenação bem definida no contexto das indeterminadas como sendo $X_1 < X_2 < \ldots < X_\ell$. Dado $e \in \mathcal{D}_j(\mathcal{C})$, com $1 \leq j \leq \ell$, considere*

$$m(\pi_1(e)) = |C_{n_1}(e_1)|$$

e, supondo $m(\pi_t(e))$ definido para $1 \leq t \leq j-1$, defina

$$\gamma_{t+1}(e) = \prod_{i=1}^{t} m(\pi_i(e)) \text{ e } m(\pi_{t+1}(e)) = \left| C_{(q^{\gamma_{t+1}(e)},\ n_{t+1})}(e_{t+1}) \right| .$$

Finalmente, para $e \in \mathcal{D}(\mathcal{C})$, definimos:

$$\gamma_{\ell+1}(e) = \prod_{j=1}^{\ell} m(\pi_j(e)).$$

Também, convencionamos $\gamma_1(e) = 1$.

Observação 2.4.6. Para $t = 1$,

$$m(\pi_1(e)) = |C_{n_1}(e_1)| = \gamma_2(e) \text{ e } m(\pi_2(e)) = |C_{(q^{\gamma_2(e)},n_2)}(e_2)|.$$

Para $t = 2$,

$$\gamma_3(e) = \gamma_2(e)m(\pi_2(e)) \text{ e } m(\pi_3(e)) = \left|C_{(q^{\gamma_3(e),n_3}(e_3)}\right|.$$

E, de modo geral,

$$\gamma_{t+1}(e) = \gamma_t(e)\left|C_{(q^{\gamma_t(e)},n_t)(e_t)}\right|.$$

Assim,

$$\frac{\gamma_{t+1}}{\gamma_t} = m(\pi_t(e)). \tag{2.1}$$

Proposição 2.4.7. *Para cada* $1 \leq t \leq \ell - 1$, *temos*

$$\gamma_{t+1}(e) = |\mathcal{O}(\pi_t(e))| = |\mathcal{O}(e_1, \ldots, e_t)| = mmc(|C_{n_1}(e_1)|, \ldots, |C_{n_t}(e_t)|).$$

Demonstração. Por indução sobre $t \geq 1$. Para $t = 1$ o resultado é imediado, pois $\gamma_2(e) = m(\pi_1(e)) = |C_{n_1}(e_1)|$. Agora, suponha que o resultado seja verdadeiro para $t \geq 1$ e vejamos que também o é para $t + 1$. Com efeito, $\gamma_{t+1}(e) = \gamma_t(e)|C_{(q^{\gamma_t(e)},n_t)}(e_t)|$. Assim, pela hipótese de indução,

$$\gamma_{t+1}(e) = mmc(|C_{n_1}(e_1)|, \ldots, |C_{n_{t-1}}(e_{t-1})|)|C_{(q^{\gamma_t(e)},n_t)}(e_t)|.$$

Denotemos por $\lambda_i = |C_{n_i}(e_i)|$, para cada $1 \leq i \leq t$, $\lambda = mmc(\lambda_1, \ldots, \lambda_t)$ e por $\beta = |C_{(q^{\gamma_t(e)},n_t}(e_t)|$. Uma vez que

$$e_t(q^{\gamma_t(e)})^\beta \equiv e_t(mod\ n_t),$$

tem-se $\lambda_t \mid \gamma_t(e)\beta$. Também, como $\lambda_i \mid \gamma_t(e)$, para cada $1 \leq i \leq t - 1$, resulta $\lambda_i \mid \gamma_t(e)\beta$. Agora, suponha que fosse possível escrever $\lambda = \gamma_t(e)\theta$, com $\theta < \beta$. Então, por um lado, $e_t q^\lambda \equiv e_t \pmod{n_t}$ e, por outro lado, $e_t q^{\gamma_t(e)\theta} \equiv e_t(mod\ n_t)$ com $\theta < \beta$, isto daria uma contradição com a minimalidade de β, isto é, $\theta \geq \beta$ e, consequentemente, $\lambda \geq \gamma_t(e)\beta$. Como já tínhamos que $\gamma_t(e)\beta \geq \lambda$, segue, $\lambda = \gamma_t(e)\beta$, como desejávamos. □

Uma vez que um elemento $e \in \mathcal{D}(\mathcal{C})$ é um representante de uma q-órbita poderíamos nos perguntarmos se os parâmetros acima permanecem os mesmos independentemente da particular escolha dos representantes de classes. De fato, isso ocorre. Para comprovarmos isso, precisaremos antes do seguinte lema:

Lema 2.4.8. *Sejam $q = p^k$, p primo, e $n \in \mathbb{N}$ tal que $p \nmid n$. Se $s, s' \in \mathbb{N}$ são tais que $C_n(s) = C_n(s')$, então $|C_{(q^\gamma,n)}(s)| = |C_{(q^\gamma,n)}(s')|$, para cada $\gamma \in \mathbb{N}$.*

Demonstração. De fato, defina

$$\begin{array}{rccc} f: & C_{(q^\gamma,n)}(s) & \to & C_{(q^\gamma,n)}(s') \\ & sq^{\gamma k_1} & \mapsto & s'q^{\gamma k_1} \end{array}$$

e vejamos que f é uma bijeção. Primeiramente, mostremos que f é bem definida. Para tanto, consideramos $r = |C_n(s)| = |C_n(s')|$ e $sq^{\gamma k_1} \equiv sq^{\gamma k_2} (mod\ n)$. Suponha, sem perda de generalidade, que $k_2 < k_1$, então

$$\begin{aligned} sq^{\gamma(k_1-k_2)} \equiv s \pmod n &\iff r \mid \gamma(k_1 - k_2) \\ &\iff s'q^{\gamma(k_1-k_2)} \equiv s' \pmod n \\ &\iff s'q^{\gamma k_1} \equiv s'q^{\gamma k_2} \pmod n \\ &\iff f(sq^{\gamma k_1}) = f(sq^{\gamma k_2}). \end{aligned}$$

Em particular, f é injetiva. Por fim, dado $y = s'q^{\gamma k} \in C_{(q^\gamma,n)}(s')$, tome $x = s'q^{\gamma k} \in C_{(q^\gamma,n)}(s)$ e note que $f(x) = y$, isto é, f é sobrejetiva. Portanto, f é uma bijeção. □

Proposição 2.4.9. *Os parâmetros $m(\pi_t(e))$ e $\gamma_{t+1}(e)$ não dependem da particular escolha do representante da classe de $e \in \mathcal{D}(\mathcal{C})$, isto é, se e, e' são representantes da mesma q-classe ciclotômica módulo $(n_1, \ldots, n_\ell)$, então $m(\pi_t(e)) = m(\pi_t(e'))$ e $\gamma_{t+1}(e) = \gamma_{t+1}(e')$.*

Demonstração. Inicialmente, se

$$e = (e_1, \ldots, e_\ell), e' = (e'_1, \ldots, e'_\ell) \in \mathcal{D}(\mathcal{C})$$

são representantes de uma mesma classe, então existe $k \in \mathbb{N}$ tal que:

$$e_j \equiv e'_j q^k (mod\ n_j), \forall j = 1, \ldots, \ell.$$

Em particular, $C_{n_j}(e_j) = C_{n_j}(e'_j)$. Agora, provemos a proposição por indução sobre $t \geq 1$. Para $t = 1$ a proposição é trivialmente satisfeita, visto que $m(\pi_1(e)) = |C_{n_1}(e_1))| = |C_{n_1}(e'_1)| = m(\pi_1(e'_1))$. Suponha, por hipótese de indução, que o resultado seja verdadeiro. Para cada $1 \leq t < \ell$ e vejamos que também é para $t + 1$. De fato, pela hipótese, segue-se que

$$\gamma_{t+1}(e) = \prod_{j=1}^{t} m(\pi_j(e)) = \gamma_{t+1}(e').$$

Deste modo, devido ao Lema 2.4.8, temos

$$\left|C_{(q^{\gamma_{t+1}(e)},n_{t+1})}(e_{t+1})\right| = \left|C_{(q^{\gamma_{t+1}(e)},n_{t+1})}(e'_{t+1})\right|,$$

isto é, $m(\pi_{t+1}(e)) = m(\pi_{t+1}(e'))$. □

Definição 2.4.10. *Sejam $\mathcal{C} \subset \mathcal{A}(n_1, \ldots, n_\ell)$ um código abeliano com conjunto definidor $\mathcal{D}(\mathcal{C})$. Um subconjunto $L \subset \mathcal{D}(\mathcal{C})$ é um* ***conjunto de representantes*** *de q-órbitas para $\mathcal{D}(\mathcal{C})$ se $\mathcal{D}(\mathcal{C}) = \dot{\bigcup}_{e\in L} \mathcal{O}(e)$. Ainda, se para $e = (e_1, \ldots, e_\ell)$, $e' = (e'_1, \ldots, e'_\ell)$ em L tais que:*

1. *$\gamma_t(e) = \gamma_t(e')$;*
2. *e_t, e'_t pertencem a mesma $q^{\gamma_t(e)}$-classe ciclotômica módulo n_t*

implicar $e_t = e'_t$, então dizemos que L é um ***conjunto completo de representantes restritos*** *e denotamos $L = \overline{\mathcal{D}}(\mathcal{C})$.*

Agora, construiremos o conjunto $\overline{\mathcal{D}}(\mathcal{C})$ a partir do conjunto $\mathcal{D}(\mathcal{C})$ por recorrência como segue:

Primeiramente, tomamos um conjunto completo de representantes de q-classes ciclotômicas módulo n_1 para os elementos de $D_1(\mathcal{C}) = \pi_1(\mathcal{D}(\mathcal{C}))$, q denotamos por $\overline{\mathcal{D}}_1(\mathcal{C})$. Agora, suponha que tenhamos definido $\overline{\mathcal{D}}_j(\mathcal{C})$ para cada $1 \leq j < i < \ell$. Dado $e \in \overline{\mathcal{D}}_{i-1}(\mathcal{C})$ definimos $\overline{\mathcal{D}}_i(e)$ como sendo o conjunto de todos os elementos da forma $(e, a_i) = (e_1, \ldots, e_{i-1}, a_i)$ em que a_i percorre um conjunto completo de $q^{\gamma_i(e)}$-classes ciclotômicas módulo n_i dos elementos do conjunto $D_i(e) = \{a \in \mathbb{Z}_{n_i} \mid (e, a) \in \mathcal{D}_i(\mathcal{C})\}$. Também, se $e, e' \in \overline{\mathcal{D}}_{i-1}(\mathcal{C})$ e $\gamma_i(e) = \gamma(e')$ então tomamos os mesmos representantes em cada $q^{\gamma_i(e)}$-classe ciclotômica em $\mathcal{D}_i(e) \cap \mathcal{D}_i(e')$. Considere,

$$\overline{\mathcal{D}}_i(\mathcal{C}) = \bigcup_{e\in\overline{\mathcal{D}}_{i-1}(\mathcal{C})} \overline{\mathcal{D}}_i(e).$$

Finalmente, definimos $\overline{\mathcal{D}}(\mathcal{C}) = \overline{\mathcal{D}}_\ell(\mathcal{C})$.

Construção de $\Gamma(\mathcal{C})$

Para cada $i = 1, \ldots, \ell - 1$, denotamos por $\overline{\mathcal{D}}_i(\mathcal{C})$ a imagem da $\overline{\mathcal{D}}(\mathcal{C})$ pela projeção π_i Fixado $e = (e_1, \ldots, e_i) \in \overline{\mathcal{D}}_i(\mathcal{C})$, considere:

$$R(e) = \{a \in \mathbb{Z}_{n_{i+1}} : (e, a) \in \overline{\mathcal{D}}_{i+1}(\mathcal{C})\}.$$

Em que, $(e, a) =: (e_1, \ldots, e_i, a)$. Também, para cada $e \in \overline{\mathcal{D}}_{\ell-1}(\mathcal{C})$, defina:

$$M(e) = \sum_{a \in R(e)} m(e, a), \tag{2.2}$$

com

$$m(e, a) = m(e_1, \ldots, e_{l-1}, a) = \left| C_{(q^{\gamma_\ell(e,a)}, n_\ell)(a)} \right|.$$

Consideramos o conjunto de todas as possíveis somas $\{M(e)\}_{e \in \overline{\mathcal{D}}_{\ell-1}(\mathcal{C})}$. Agora, definiremos alguns parâmetros a partir dos valores $M(e)'s$. Seja

$$f[1] = \max_{e \in \overline{\mathcal{D}}_{\ell-1}(\mathcal{C})} \{M(e)\}$$

e

$$f[i] = \max_{e \in \overline{\mathcal{D}}_{\ell-1}(\mathcal{C})} \{M(e); M(e) < f[i-1]\}.$$

Assim, obtemos uma sequência estritamente decrescente:

$$f[1] > ... > f[s_\ell] > 0 = f[s_\ell + 1]$$

Em que convencionamos $f[s_\ell + 1] = 0$, com s_ℓ correspondendo ao número de parâmetros $M(-)$ que são distintos e não nulos, isto é, $s_\ell = |\{M(e)_{e \in \overline{\mathcal{D}}_{\ell-1}(\mathcal{C})}\}|$.

Agora, suponha $\ell \geq 3$. Dados arbitrariamente $1 \leq u_\ell \leq s_\ell$ e $e \in \overline{\mathcal{D}}_{\ell-2}(\mathcal{C})$ definimos:

$$\Omega_{u_\ell}(e) = \{a \in R(e); M(e, a) \geq f[u_\ell]\}.$$

Note que, podemos calcular $M(e, a)$, visto que $(e, a) \in \overline{\mathcal{D}}_{l-1}(\mathcal{C})$. Também, definimos

$$\mu_{u_\ell}(e) = \sum_{a \in \Omega_{u_\ell}(e)} m(e, a).$$

Se, eventualmente, tivermos $\Omega_{u_\ell} = \varnothing$, convencionamos $\mu_{u_\ell}(e) = 0$. Defina

$$f[u_\ell, 1] = \max_{e \in \overline{\mathcal{D}}_{\ell-2}(\mathcal{C})} \{\mu_{u_\ell}(e)\}$$

e

$$f[u_\ell, i] = \max_{e \in \overline{\mathcal{D}}_{\ell-2}(\mathcal{C})} \{0 < \mu_{u_\ell} < f[u_\ell, i-1]\}.$$

Assim, para cada $1 \leq u_\ell \leq s_n$, obtemos uma sequência:

$$f[u_\ell, 1] > \ldots > f[u_\ell, s(u_\ell)] > 0 = f[u_\ell, s(u_\ell) + 1],$$

qual, novamente, convencionamos que $f[u_\ell, s(u_\ell)+1] = 0$. Aqui $s(u_\ell)$ denota o número de parâmetros μ_{u_ℓ} distintos e não nulos. Note que a notação $s(-)$ é abusiva uma vez que, em geral, tais parâmetros não dependem da sequência anterior.

Agora, suponha que $l \geq j \geq 4$ e que, para cada sequência $(u_\ell, \ldots, u_j)$, em que $1 \leq u_\ell \leq s_\ell$ e $1 \leq u_i \leq s(u_\ell, \ldots, u_{i+1})$, com $j \leq i < \ell$, tenhamos construído a sequência

$$f[u_\ell, \ldots, u_j, 1] > \ldots > f[u_\ell, \ldots, u_j, s(u_\ell, \ldots, u_j)] > 0 = f[u_\ell, \ldots, u_j, s(u_\ell, \ldots, u_j)+1].$$

Então, definimos para cada $e \in \overline{\mathcal{D}}_{j-3}(\mathcal{C})$ e $1 \leq u_{j-1} \leq s(u_\ell, \ldots, u_j)$,

$$\Omega_{u_\ell,\ldots,u_{j-1}(e)} = \{a \in R(e) : \mu_{u_\ell,\ldots,u_j}(e,a) \geq f[u_\ell, \ldots, u_j, u_{j-1}]\}$$

e

$$\mu_{u_\ell,\ldots,u_{j-1}}(e) = \sum_{a \in \Omega_{u_\ell,\ldots,u_{j-1}(e)}} m(e,a),$$

e ordenando esses parâmetros obtemos uma sequência:

$$f[u_\ell, \ldots, u_{j-1}, 1] > \ldots > f[u_\ell, \ldots, u_{j-1}, s(u_\ell, \ldots, u_{j-1})] > 0 = f[u_\ell, \ldots, u_j - 1, s(u_\ell, \ldots, u_{j-1})+1].$$

Continuamos dessa forma a até termos definido, para cada $(u_\ell, \ldots, u_3)$, a sequência

$$f[u_\ell, \ldots, u_3, 1] > \ldots > f[u_\ell, \ldots, u_3, s(u_\ell, \ldots, u_3)] > 0 = f[u_\ell, \ldots, u_j - 1, s(u_\ell, \ldots, u_3)+1].$$

Finalmente, para qualquer valor de ℓ, definimos a última lista de parâmetros $(u_\ell, \ldots, u_2)$, com $1 \leq u_\ell \leq s_\ell$ e $1 \leq u_i \leq s(u_\ell, \ldots, u_{i+1})$, onde $2 \leq i < \ell$. Se $\ell = 2$, defina

$$g[u_2] = \sum_{\substack{e \in \overline{\mathcal{D}}_1(\mathcal{C}) \\ M(e) \geq f[u_2]}} m(e).$$

O caso em que $\ell > 2$, definimos:

$$g[u_\ell, \ldots, u_2] = \sum_{\substack{e \in \overline{\mathcal{D}}_1(\mathcal{C}) \\ \mu_{(u_\ell,\ldots,u_3)}(e) \geq f[u_\ell,\ldots,u_2]}} m(e).$$

Usando as sequências obtidas anteriormente, podemos definir o conjunto:

$$\Gamma(\mathcal{C}) = \Big\{(i_1,\ldots,i_\ell) \in \prod_{i=1}^{\ell} \mathbb{Z}_{n_i} : \exists (u_\ell,\ldots,u_2),\ \text{com}$$
$$1 \leq u_\ell \leq s_\ell,$$
$$1 \leq u_i \leq s(u_\ell,\ldots,u_{i+1}), \forall i = 2,\ldots,\ell-1;$$
$$\text{tal que}$$
$$f[u_\ell+1] \leq i_\ell < f[u_\ell],$$
$$\ldots,$$
$$f[u_\ell,\ldots,u_2+1] \leq i_2 < f[u_\ell,\ldots,u_2],$$
$$0 \leq i_1 < g[u_\ell,\ldots,u_2]\Big\}.$$

O resultado principal desse estudo é provar que o conjunto $\Gamma(\mathcal{C}) \subset \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell}$, é um **conjunto posições de verificação**, o que será feito no próximo capítulo.

Observação 2.4.11.

1. Para o caso em que $\ell = 2$, pode-se verificar que o conjunto

   $$\Gamma(\mathcal{C}) = \{(i_1,i_2) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} : \exists u \in \{1,\ldots,s_n\} \text{ com } f[u+1] \leq i_2 < f[u] \text{ e } 0 \leq i_1 < g[u]\}$$

   construído por Imai, em [8], para códigos TDC, é um conjunto de posições de verificação visto sob outras notações.

2. A construção do conjunto $\Gamma(\mathcal{C})$ depende unicamente dos valores $m(-)$ calculados sobre um conjunto de representantes restritos e, como constatamos na Proposição 2.4.9, esses valores são independentes dos representantes escolhidos, desde que sua escolha respeite à restrição imposta. Portanto, qualquer escolha de representantes restritos produz o mesmo conjunto verificador de posições desde que a ordem das indeterminadas esteja fixada.

O próximo resultado nos dá com precisão o número de elementos de $\Gamma(\mathcal{C})$.

Proposição 2.4.12. *Sejam $\Gamma(\mathcal{C})$ o subconjunto de $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_\ell}$ obtido como acima, Υ o conjunto de todas as sequências obtidas na construção de $\Gamma(\mathcal{C})$ e $u = (u_\ell,\ldots,u_2)$ uma*

sequência qualquer em Υ*. Então,*

$$|\Gamma(\mathcal{C})| = \sum_{u\in\Upsilon}(f[u_\ell] - f[u_\ell+1]) \cdot \ldots \cdot (f[u_\ell,\ldots,u_2] - f[u_\ell,\ldots,u_2+1])(g[u_\ell,\ldots,u_2]) \tag{2.3}$$

Demonstração. Inicialmente, note que $i = (i_1,\ldots,i_\ell) \in \Gamma(\mathcal{C})$ se, e somente se, existe $u \in \Upsilon$ com $1 \leq u_\ell < s_\ell$ e $1 \leq u_i \leq s(u_\ell,\ldots,u_{i+1})$ com $i = 2,\ldots,\ell-1$, de modo que

$$f[u_\ell+1] \leq i_\ell < f[u_\ell],\ldots,f[u_\ell,\ldots,u_2+1] \leq i_2 < f[u_\ell,\ldots,u_2] \text{ e } 0 \leq i_1 < g[u_\ell,\ldots,u_2].$$

Assim, para cada $u \in U$, temos

$$\begin{array}{cc} f[u_\ell] - f[u_\ell+1] & \text{possibilidades para } i_\ell \\ \vdots & \vdots \\ f[u_\ell,\ldots,u_2] - f[u_\ell,\ldots,u_2+1] & \text{possibilidades para } i_2 \\ g[u_\ell,\ldots,u_2] & \text{possibilidades para } i_1 \end{array}$$

Logo, temos $(f[u_\ell] - f[u_\ell+1]) \cdot \ldots \cdot (f[u_\ell,\ldots,u_2] - f[u_\ell,\ldots,u_2+1])g[u_\ell,\ldots,u_2]$ possibilidades para i. Deste modo, a igualdade em (2.3) estará estabelecida se provarmos que para sequências u e u' distintas, os elementos $i \in \Gamma(\mathcal{C})$ obtidos a partir das restrições de u nunca podem ser obtidos pelas restrições dadas por u'. Para ver isso, considere $u = (u_\ell,\ldots,u_2) \neq u' = (u'_\ell,\ldots,u'_2)$ e seja j o maior índice tal que $u_j \neq u'_j$. Caso $j = \ell$, podemos supor, sem perda de generalidade, que $u_\ell < u'_\ell$. Então, $f[u'_\ell] < f[u_\ell]$. Ainda, se $i = (i_1,\ldots,i_\ell)$ é obtido a partir das restrições de u, deve valer

$$f[u'_\ell+1] \leq i_\ell < f[u'_\ell] \Rightarrow f[u'_\ell] \leq f[u_\ell+1] \leq i_\ell.$$

Assim, neste caso, nenhum elemento obtido por u pode ser obtido por u', pois, se isso fosse possível, deveríamos ter

$$f[u'+1] \leq i_\ell < f[u'_\ell] \leq f[u'_\ell+1] \leq i_\ell < f[u'_\ell]$$

o que é impossível. Caso $j < \ell$, isto é, para cada $k > j$, $u_k = u'_k$ e $u_j \neq u'_j$. Novamente podemo supor, sem perda da generalidade, que $u_j < u'_j$. Assim, se $i = (i_1,\ldots,i_\ell) \in \Gamma(\mathcal{C})$ é obtido pela restrição de u então:

$$f[u_\ell,\ldots,u'_j+1] \leq i_j < f[u_\ell,\ldots,u'_j] \leq f[u_\ell,\ldots,u_j+1],$$

implicando que a j-ésima upla de i difere na j-ésima upla de qualquer elemento obtido por u e, portanto o resultado fica provado. □

Observação 2.4.13. Note que, ao invés de escrever

$$\sum_{u=(u_\ell,\ldots,u_2)} (f[u_\ell]-f[u_\ell+1])\cdot\ldots\cdot(f[u_\ell,\ldots,u_2]-f[u_\ell,\ldots,u_2+1])(g[u_\ell,\ldots,u_2]), \quad (2.4)$$

deveríamos escrever, mais rigorosamente,

$$\sum_{u_\ell=1}^{s_\ell}\sum_{u_{\ell=1}}^{s(u_\ell)}\cdots\sum_{u_2=1}^{s(u_\ell,\ldots,u_3)} (f[u_\ell]-f[u_\ell+1])\cdot\ldots\cdot(f[u_\ell,\ldots,u_2]-f[u_\ell,\ldots,u_2+1])(g[u_\ell,\ldots,u_2])$$

deixando claro os intervalos de variação dos parâmetros u_i. Porém, adotaremos a expressão em (2.4) de modo a simplificar a notação.

Assuma, por um instante, que $\Gamma(\mathcal{C})$ é um conjunto de posições de verificações. Antes de provar o teorema principal desse estudo, veremos alguns casos particulares juntamente com alguns exemplos.

Primeiramente, abordaremos o caso em que $n = n_1n_2$ com $mdc(n_1, n_2) = 1$. Assim, $\mathbb{Z}_n \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ como grupos. Ainda, existe um isomorfismo $\mu : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ obtido pelo Teorema Chinês do Resto. Além disso, devido ao Corolário 2.1.7, podemos considerar a extensão de μ, a um isomorfismo de $\mathbb{F}$-álgebras, $\overline{\mu} : \mathcal{A}(n) \to \mathcal{A}(n_1, n_2)$. O isomorfismo μ possui a seguinte propriedade:

Proposição 2.4.14. *Sejam $n = n_1n_2$ com $mdc(n_1, n_2) = 1$ e $\overline{\mu} : \mathcal{A}(n) \to \mathcal{A}(n_1, n_2)$ o isomorfismo obtido pelo Teorema Chinês do Resto. Se $\mathcal{C} \subset \mathcal{A}(n)$ é um código cíclico, então $\overline{\mu}(\mathcal{C})$ é um código abeliano em $\mathcal{A}(n_1, n_2)$. Além disso, se $\mathcal{D}(\mathcal{C})$ é o conjunto definidor de $\mathcal{C}$, temos $\mu(\mathcal{D}(\mathcal{C})) = \mathcal{D}(\overline{\mu}(\mathcal{C}))$.*

Demonstração. Como $\overline{\mu}$ é um isomorfismos de $\mathbb{F}_q$-álgebras e $\mathcal{C}$ é um ideal de $\mathcal{A}(n)$ segue-se que $\mu(\mathcal{C})$ é um ideal de $\mathcal{A}(n_1, n_2)$ e, portanto, um código abeliano. Resta ver a igualdade $\mathcal{D}(\overline{\mu}(\mathcal{C})) = \mu(\mathcal{D}(\mathcal{C}))$. Para $r \in \mathbb{Z}$ denotamos por $[r]_n \in \mathbb{Z}_n$ o representante canônico da classe r módulo n, então dado $a \in \mathbb{Z}_n$, temos

$$\mu(a) = ([a]_{n_1}, [a]_{n_2}).$$

Logo, se $p(X) = \sum_{i=0}^{n-1} p_iX^i \in \mathcal{A}(n)$, então:

$$\overline{\mu}\left(\sum_{i=0}^{n-1} p_iX^i\right) = \sum_{i=0}^{n-1} q_{[i]_{n_1},[i]_{n_2}} X_1^{[i]_{n_1}} X_2^{[i]_{n_2}}$$

em que $q_{[i]_{n_1},[i]_{n_2}} = p_i$. Seja α um n-ésima raiz primitiva da unidade. Sabemos que existem, para $i = 1, 2$, raízes n_i-ésima primitivas da unidade, α_i tais que $\alpha = \alpha_1\alpha_2$ e, além disso, dado $a \in \mathbb{Z}_n$, tem-se:

$$\alpha^a = \alpha_1^{[a]_{n_1}} \alpha_2^{[a]_{n_2}}. \tag{2.5}$$

Lembremos que, as q-órbitas em $\mathbb{Z}_n$ são as q-classes ciclotômicas módulo n, isto é, $\mathcal{O}(a) = \{aq^i : i \in \mathbb{N}\} \subset \mathbb{Z}_n$ Também, devido a (2.5), temos que:

$$\mu(\mathcal{O}(a)) = \mathcal{O}([a]_{n_1}, [a]_{n_2}) = \mathcal{O}(\mu(a)).$$

Agora, note que $\mu(\mathcal{D}(\mathcal{C}))$ é reunião de q-órbitas. De fato, existe um conjunto L de representantes de q-orbitas módulo n para $\mathcal{C}$, tal que:

$$\mathcal{D}(\mathcal{C}) = \bigcup_{a \in L} \mathcal{O}(a).$$

Deste modo,

$$\mu(\mathcal{D}(\mathcal{C})) = \mu\left(\bigcup_{a \in L} \mathcal{O}(a)\right) = \bigcup_{a \in L} \mu(\mathcal{O}(a)) = \bigcup_{a \in L} (\mathcal{O}(\mu(a)).$$

Assim, $\mu(\mathcal{D}(\mathcal{C}))$ é reunião de q-órbitas. Finalmente, veja que:

$$\begin{aligned} p(\alpha^a) &= \sum_{i=0}^{n-1} p_i \alpha^{ai} \\ &= \sum_{i=0}^{n-1} p_i \alpha_1^{[ai]_{n_1}} \alpha_2^{[ai]_{n_2}} \\ &= \sum_{i=0}^{n-1} q_{[i]_{n_1},[i]_{n_2}} \alpha_1^{[ai]_{n_1}} \alpha_2^{[ai]_{n_2}} q_{[i]_{n_1},[i]_{n_2}} \\ &= \overline{\mu}(p)(\alpha_1^{[a]_{n_1}} \alpha_2^{[a]_{n_2}}). \end{aligned}$$

Com isso, $a \in \mathcal{D}(\mathcal{C})$ se, e somente se, $\mu(a) \in \mathcal{D}(\overline{\mu}(\mathcal{C}))$ e, portanto, o resultado segue. □

Assim, podemos calcular um conjunto de informações para $\overline{\mu}(\mathcal{C})$ e então tomar a imagem inversa dessas posições por μ, obtendo um novo conjunto de informações para $\mathcal{C}$.

Vejamos um exemplo:

Exemplo 2.4.15. Considere $\mathcal{C}$ o código cíclico binário de comprimento 15 dado pelo conjunto de raízes:

$$\mathcal{Z}(\mathcal{C}) = \{\alpha^e : e = 0, 1, 2, 3, 4, 6, 8, 9, 12\}$$

Observe que $\mathcal{Z}(\mathcal{C})$ realmente define um código cíclico sobre $\mathbb{F}_2$, pois:

$$\mathcal{D}(\mathcal{C}) = \{0,1,2,3,4,6,8,9,12\} = C_{(2,15)}(0) \cup C_{(2,15)}(1) \cup C_{(2,15)}(3)$$

é reunião de 2-classes ciclotômicas. Usando o Teorema Chinês do Resto, definimos o isomorfismo

$$\begin{array}{rccc} \mu: & \mathbb{Z}_{15} & \to & \mathbb{Z}_3 \times \mathbb{Z}_5 \\ & t & \mapsto & (t_1, t_2) \end{array}$$

de modo que $t_1 \equiv t(mod\ 3)$ e $t_2 \equiv t(mod\ 5)$. Considerando α_1 uma raiz cúbica da unidade e α_2 uma raiz quinta da unidade, temos $\alpha = \alpha_1\alpha_2$ e obtemos:

$$\mathcal{Z}(\overline{\mu}(\mathcal{C})) = \{(1,1),(\alpha_1,\alpha_2),(\alpha_1^2,\alpha_2^2),(1,\alpha_2^3),(\alpha_1,\alpha_2^4),(1,\alpha_2),(\alpha_1^2,\alpha_2^3),(1,\alpha_2^4),(1,\alpha_2^2)\}$$

Uma vez que

$$\begin{aligned} \mathcal{D}(\overline{\mu}(\mathcal{C})) =& \{\mu(0) = (0,0), \mu(1) = (1,1), \mu(2) = (2,2), \mu(3) = (0,3), \mu(4) = (1,4), \\ & \mu(6) = (0,1), \mu(8) = (2,3), \mu(9) = (0,4), \mu(12) = (0,2)\}. \end{aligned}$$

Agora construiremos um conjunto completo de representantes para $\mathcal{D}(\overline{\mu}(\mathcal{C}))$. Note que $\overline{D}_1(\mathcal{C}) = \{0,1\}$ é um conjunto completo de representantes de 2-classes ciclotômicas módulo 3 para $\mathcal{D}_1(\mathcal{C}) = \{0,1,2\}$. Como $\gamma_2(0) = \left|C_{(2,3)}(0)\right| = |\{0\}| = 1$ e $D_2(0) = \{(0,0),(0,3),(0,1),0,2),(0,4)\}$ resulta $\overline{\mathcal{D}}_2(0) = \{(0,0),(0,1)\}$, uma vez que $2,3,4 \in C_{(2^{\gamma_2(0)},5)}(1) = C_{(2,5)}(1)$. Por outro lado, $D_2(1) = \{(1,1),(1,4)\}$ sendo $C_{(2,3)}(1) = \{1,2\}$, temos, $\gamma_2(1) = 2$ e $C_{(2^{\gamma_2(1)},5)}(1) = C_{(2^2,5)}(1) = \{1,4\}$ de onde $\overline{D}_2(1) = \{(1,1)\}$. Logo,

$$\overline{\mathcal{D}}(\overline{\mu}(C)) = \overline{\mathcal{D}}_2(0) \cup \overline{D}_2(1) = \{(0,0),(0,1),(1,1)\}$$

é um conjunto de representantes restritos e é a partir deste que obteremos os valores $f[-]$ e $g[-]$ para então definir $\Gamma(\overline{\mu}(\mathcal{C}))$. Como $\overline{\mathcal{D}}_1(\mathcal{C}) = \{0,1\}$, temos

$$\begin{aligned} & R(0) = \{0,1\},\ M(0) = m(0,0) + m(0,1) \text{ e} \\ & R(1) = \{1\},\ M(1) = m(1,1) \end{aligned}$$

em que $m(i,j) = \left|C_{(2^{\gamma_2(i,j)},5)}(j)\right|$. Assim,

$$m(0,0) = \left|C_{(2,5)}(0)\right| = 1,\ m(0,1) = \left|C_{(2,5)}(1)\right| = 4 \text{ e } m(1,1) = \left|C_{(2^2,5)}(1)\right| = 2,$$

então $M(0) = 5$ e $M(1) = 2$. Deste modo,

$$f[1] = \max\{M(0), M(1)\} = 5,\ f[2] = 2, f[3] = 0,$$
$$g[1] = \sum_{\substack{e \in \overline{\mathcal{D}}_1(\mathcal{C}) \\ M(e) \geq f[1]}} m(e) = 1 \text{ e } g[2] = \sum_{\substack{e \in \overline{\mathcal{D}}_1(\mathcal{C}) \\ M(e) \geq f[2]}} m(e) = m(0) + m(1) = 3.$$

Portanto,

$$\begin{aligned}\Gamma(\overline{\mu}(\mathcal{C})) &= \{(i_1, i_2) \in \mathbb{Z}_3 \times \mathbb{Z}_5 : \exists u \in \{1, 2\} \text{ com } f[u+1] \leq i_2 < f[u] \text{ e } 0 \leq i_1 < g[u]\} \\ &= \{(0,2), (0,3), (0,4), (0,0), (0,1), (1,0), (1,1), (2,0), (2,1)\}\end{aligned}$$

é um conjunto de posições de verificação para $\overline{\mu}(\mathcal{C})$. Portanto,

$$\mu^{-1}(\Gamma(\overline{\mu}(\mathcal{C}))) = \{0, 1, 3, 5, 6, 9, 10, 11, 12\}$$

é um conjunto de posições de verificação para $\mathcal{C}$ que não é óbvio, isto é, diferente dos obtidos pela Proposição 1.3.8.

A Proposição 2.4.14 vale em um contexto mais geral, isto é, para um isomorfismo arbitrário não necessariamente fornecido pelo Teorema Chinês do Resto. Assim, seu enunciado fica da seguinte forma

Proposição 2.4.16. *Sejam $n = n_1 n_2$, com $mdc(n_1, n_2) = 1$, e $\psi : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ um isomorfismo de grupos. Se $\mathcal{C} \subset \mathcal{A}(n)$ é um código cíclico com conjunto definidor $\mathcal{D}(\mathcal{C})$, então $\mathcal{D}(\overline{\psi}(\mathcal{C})) = \psi(\mathcal{D}(\mathcal{C}))$.*

O seguinte lema fornece uma caracterização dos isomorfismos entre $\mathbb{Z}_n$ e $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, em que $n = n_1 n_2$ e $mdc(n_1, n_2) = 1$. Essa caraterização é extremamente útil para provar os resultados subsequentes.

Lema 2.4.17. *Sejam $n = n_1 n_2$ com $mdc(n_1, n_2) = 1$. Considere que*

$$\begin{array}{rccc} \mu: & \mathbb{Z}_n & \to & \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \\ & t & \mapsto & (t_1, t_2) \end{array}$$

é o isomorfismo obtido no Teorema Chinês do Resto. Todo isomorfismo $\psi : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ é da forma $\psi(t) = (k_1 t_1, k_2 t_2)$ com $\mu(t) = (t_1, t_2)$ para convenientes $k_i's$ fixados e invertíveis módulo n_i para $i = 1, 2$.

Demonstração. Com cálculos simples vê-se que ψ é bem definida e injetiva. Além disso, ψ é sobrejetiva, pois dado $(t_1, t_2) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ tome $x \in \mathbb{Z}_n$ tal que, $\mu(x) = (k_1^{-1}t_1, k_2^{-1}t_2)$, logo $\psi(x) = (t_1, t_2)$. Finalmente, vejamos que ψ é homomorfismo. De fato, dados $t, s \in \mathbb{Z}_n$ temos $\psi(t) = (k_1t_1, k_2t_2)$ e $\psi(s) = (k_1s_1, k_2s_2)$, com $\mu(t) = (t_1, t_2)$ e $\mu(s) = (s_1, s_2)$. Daí, sendo μ homomorfismo, tem-se $\mu(t + s) = \mu(t) + \mu(s)$. Assim,

$$\begin{aligned}\psi(t) + \psi(s) &= (k_1t_1, k_2t_2) + (k_1s_1, k_2s_2)\\ &= (k_1t_1 + k_1s_1, k_2t_2 + k_2s_2)\\ &= (k_1(t_1 + s_1), k_2(t_2 + s_2))\\ &= \psi(t + s).\end{aligned}$$

Logo, ψ é isomorfismo. Agora, lembremos que o número de isomorfismo de $\mathbb{Z}_n$ em $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ é $\varphi(n)$, em que φ denota a Função Totiente de Euler, que determina a quantidade de números relativamente primos com n que estão entre 1 e n. Como existem $\varphi(n_i)$ possibilidades para escolher do elemento invertível k_i para $i = 1, 2$, então existem $\varphi(n_1)\varphi(n_2) = \varphi(n)$ possibilidades de escolher (k_1, k_2) e cada escolha dessas da origem a um único isomorfismo. Portanto, o resultado segue. □

Observação 2.4.18. O Lema 2.4.17 e a Proposição 2.4.16 se generalizam, de modo natural, para número qualquer finito de fatores no produto cartesiano. Assim, podemos reescrevê-los como:

- Lema 2.4.17: Sejam $n = n_1 \dots n_\ell$ com $mdc(n_i, n_j) = 1$ para quaisquer $1 \leq i \neq j \leq \ell$. Considere que

$$\begin{array}{rccc}\mu: & \mathbb{Z}_n & \to & \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_\ell}\\ & t & \mapsto & (t_1, \ldots, t_\ell)\end{array}$$

  é o isomorfismo obtido no Teorema Chinês do Resto. Então, todo isomorfismo $\psi : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell}$ é da forma $\psi(t) = (k_1t_1, \ldots, k_\ell t_\ell)$ com $\mu(t) = (t_1, \ldots, t_\ell)$ para convenientes $k_i's$ fixados e invertíveis módulo n_i com $i = 1, \ldots, \ell$.

- Proposição 2.4.16: Sejam $n = n_1 \dots n_\ell$, com $mdc(n_i, n_j) = 1$, e

$$\psi : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_\ell \tag{2.6}$$

  um isomorfismo de grupos. Se $\mathcal{C} \subset \mathcal{A}(n)$ é um código cíclico com conjunto definidor $\mathcal{D}(\mathcal{C})$, então $\mathcal{D}(\overline{\psi}(\mathcal{C})) = \psi(\mathcal{D}(\mathcal{C}))$.

Proposição 2.4.19. *Considere $n = n_1...n_\ell$ um inteiro positivo tal que, $n_1, ..., n_\ell$ são dois a dois coprimos, então existe um isomorfismo de grupos:*

$$\psi : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_\ell}$$

Sejam $\mathbb{F}_q$ um corpo de característica coprima com n e $\mathcal{C} \subset \mathcal{A}(n)$ um código cíclico, temos:

1) Se L é um conjunto completo de representantes de q-classes ciclotômicas módulo n para $\mathcal{C}$ então:

$$D(\overline{\psi}(\mathcal{C})) = \psi(D(\mathcal{C})) = \psi(\bigcup_{s\in L} C_n(s)) = \bigcup_{s\in L} \mathcal{O}(\psi(s)).$$

2) Se $\psi' : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_\ell}$ é um qualquer isomorfismo de grupos, então $m(\pi_t(\psi(s)) = m(\pi_t(\psi'(s)))$ e $\gamma_t(\psi(s)) = \gamma_t(\psi'(s))$ para cada $t = 1, ..., \ell$, isto é, os parâmetros $m(-)$ e $\gamma(-)$ são invariantes por isomorfismo.

Demonstração. Uma vez que L é um conjunto completo de q-classes ciclotômicas para $\mathcal{C}$ temos $\mathcal{D}(\mathcal{C}) = \bigcup_{s\in L} C_n(s)$. Logo,

$$\psi(\mathcal{D}(\mathcal{C})) = \psi(\bigcup_{s\in L} C_n(s)) = \bigcup_{s\in L} \psi(C_n(s)).$$

Assim, para provaro item 1, basta ver que $\psi(C_n(s)) = \mathcal{O}(\psi(s))$. De fato, como todo isomorfismo de grupos é, em particular, um $\mathbb{Z}$-isomorfismo, segue

$$\psi(C_n(s)) = \psi(\{sq^j (mod\ n) : j \in \mathbb{Z}\}) = \{\psi(sq^j) : j \in \mathbb{Z}\} = \{q^j\psi(s) : j \in \mathbb{Z}\} = \mathcal{O}(\psi(s))$$

Observe que, em particular, $|C_n(s)| = |\mathcal{O}(\psi(s))|$. Para mostrar o item 2, lembremos que:

$$\frac{\gamma_{t+1}(e)}{\gamma_t(e)} = m(\pi_t(e)), \forall e \in \mathcal{D}(\mathcal{C}), \tag{2.7}$$

e

$$\gamma_{t+1}(e) = |\mathcal{O}(e_1, \ldots, e_t)| = mmc(|C_{n_1}(e_1)|, \ldots, |C_{n_t}(e_t)|), \forall e \in \mathcal{D}(\mathcal{C}), \tag{2.8}$$

para cada $t = 1, \ldots, \ell$. Veja a Proposição 2.4.7. Agora, denote

$$\psi(s) = (k_1 s_1, \ldots, k_\ell s_\ell) \text{ e } \psi'(s) = (k'_1 s_1, \ldots, k'_\ell s_\ell),$$

com os k_i, k_i' obtidos como no Lema 2.4.17. Considere $r_i = |C_{n_i}(k_i s_i)|$ e $r_i' = |C_{n_i}(k_i' s_i)|$ e mostremos que $r_i = r_i'$ para cada $1 \leq i \leq \ell$. De fato, considere a função auxiliar

$$\begin{array}{rccc} h_i: & C_{n_i}(k_i s_i) & \to & C_{n_i}(k_i' s_i) \\ & (k_i s_i)q^j & \mapsto & (k_i' s_i)q^j \end{array}$$

e vejamos que h_i é uma bijeção. De fato, h_i é bem definida e é injetiva, pois:

$$k_i s_i q^j = k_i s_i q^t \iff s_i q^j = s_i q^t \iff k_i' s_i q^j = k_i' s_i q^t \iff h_i(k_i s_i q^j) = h_i(k_i s_i q^t).$$

Também, é claro que h_i é sobrejetora e assim $r_i = r_i'$ para cada i. Daí, por (2.8), temos

$$\begin{aligned} \gamma_{t+1}(\psi(s)) &= |\mathcal{O}(k_1 s_1, \ldots, k_t s_t)| \\ &= mmc(r_1, \ldots, r_t) \\ &= mmc(r_1', \ldots, r_t') \\ &= |\mathcal{O}(k_1' s_1, \ldots, k_t' s_t)| \\ &= \gamma_{t+1}(\psi'(s)). \end{aligned}$$

Devido a (2.1), $m(\pi_t(\varphi(s)) = m(\pi_t(\varphi'(s)))$, para cada $t = 1, \ldots, \ell$, o que prova o item 2 e conclui a demonstração. □

Corolário 2.4.20. *Considere $n = n_1 \ldots n_\ell$, com $mdc(n_i, n_j) = 1$, $\psi, \psi' : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_\ell}$ isomorfismos de grupos e $\mathcal{C} \subset \mathcal{A}(n)$ um código cíclico. Se $\overline{\mathcal{D}}(\overline{\psi}(\mathcal{C})) = \{\psi(s_1), \ldots, \psi(s_k)\}$ é um conjunto restrito de representantes para $\overline{\psi}(\mathcal{C})$, então $\{\psi'(s_1), \ldots, \psi'(s_k)\}$ é um conjunto restrito de representantes para $\overline{\mathcal{D}}(\overline{\psi'}(\mathcal{C}))$. Em particular, $\Gamma(\overline{\psi}(\mathcal{C})) = \Gamma(\overline{\psi'}(\mathcal{C}))$.*

Demonstração. Considere que $\psi(m) = (k_1 m_1, \ldots, k_l m_l)$ e $\psi'(m) = (k_1' m_1, \ldots, k_\ell' m_\ell)$ para cada $m \in \mathbb{Z}_n$ como no Lema 2.4.17. Primeiramente, vejamos que $\{\psi'(s_1), \ldots, \psi'(s_k)\} := L$ é um conjunto completo de representantes para $\overline{\psi}(\mathcal{C})$. De fato, como $\{\psi(s_1), \ldots, \psi(s_k)\}$ é um conjunto completo, segue

$$\psi(\mathcal{D}(\mathcal{C})) = \mathcal{D}(\overline{\psi}(\mathcal{C})) = \bigcup_{i=1}^{k} \mathcal{O}(\psi(s_i)).$$

Logo, $\{s_1, \ldots, s_k\}$ é um conjunto completo de q-classes ciclotômicas para $\mathcal{C}$. Assim,

$$\mathcal{D}(\mathcal{C}) = \bigcup_{i=1}^{k} C_n(s_i) \Rightarrow \mathcal{D}(\overline{\psi'}(\mathcal{C})) = \psi(\bigcup_{i=1}^{k} C_n(s_i)) = \bigcup_{i=1}^{k} \mathcal{O}(\psi'(s_i)),$$

isto é, L é um conjunto completo de representante. Agora, vejamos que L é restrito. Para tanto, suponha que existam s_i, s_j com

$$\psi'(s_i) = (k'_1 s_{1i}, \ldots, k'_\ell s_{\ell i}) \text{ e } \psi'(s_j) = (k'_1 s_{1j}, \ldots, k'_\ell s_{\ell j})$$

e os $k'_j s$ invertíveis módulo n_j, tais que

$$\gamma_t(\psi'(s_i)) = \gamma_t(\psi'(s_j)) := \lambda \text{ e } k'_t s_{ti} \in C_{(q^\lambda, n_t)}(k'_t s_{tj}).$$

Deste modo, para mostrarmos que L é restrito, pela Definição 2.4.10, devemos mostrar que $k'_t s_{ti} = k'_t s_{tj}$. De fato,

$$\begin{aligned} k'_t s_{ti} \in C_{(q^\lambda, n_t)}(k'_t s_{tj}) \iff \exists t \in \mathbb{Z} : k'_t s_{ti} = (k'_t s_{tj}) q^{t\lambda} (mod\ n_t) &\Rightarrow s_{ti} = s_{tj} q^{t\lambda} (mod\ n_t) \\ &\Rightarrow k_t s_{ti} = k_t s_{tj} q^{t\lambda} (mod\ n_t) \\ &\Rightarrow k_t s_{ti} \in C_{(q^\lambda, n_t)}(k_t s_{tj}). \end{aligned}$$

Daí, pela Proposição 2.4.19, temos:

$$\gamma_t(\psi(s_i)) = \gamma_t(\psi(s_j)) = \lambda \text{ e } k_t s_{ti} \in C_{(q^\lambda, n_t)}(k_t s_{tj}).$$

Como $\{\psi(s_1), ..., \psi(s_k)\}$ é restrito, resulta que:

$$k_t s_{ti} = k_t s_{tj} (mod\ n_t) \Rightarrow s_{ti} = s_{tj} (mod\ n_t) \Rightarrow k'_t s_{ti} = k'_t s_{tj} (mod\ n_t).$$

Ou seja, L é restrito. Assim, uma vez que os parâmetros $m(-)$ e $\gamma(-)$ são invariantes por ψ e ψ', do que acabamos de mostrar nos dá que os parâmetros $f[-]$ e $g[-]$ também são invariantes e, deste modo, $\Gamma(\overline{\psi}(\mathcal{C})) = \Gamma(\overline{\psi'}(\mathcal{C}))$. □

Observação 2.4.21. O Corolário 2.4.20 nos diz que, independente do isomorfismo ψ, sempre obtemos o mesmo conjunto de posições de verificação ou de informações para $\overline{\psi}(C)$, qualquer que seja o código $\mathcal{C}$. O interessante é que se $\psi \neq \psi'$ são isomorfismos distintos, então pode ocorrer que tenhamos $\overline{\psi}(C) \neq \overline{\psi'}(C)$ e, consequentemente, os conjuntos definidores desses códigos devem diferir. Deste modo, usando as imagens inversas de ψ e ψ', respectivamente, obtemos conjuntos de posições de verificação distintos para o mesmo código $\mathcal{C}$. O próximo exemplo ilustra isso.

Exemplo 2.4.22. Considere o código cíclico binário dado pelo conjunto definidor $\mathcal{D}(\mathcal{C}) = \{0, 1, 2, 3, 4, 6, 8, 9, 12\}$, como no Exemplo 2.4.15, e $\varphi : \mathbb{Z}_{15} \to \mathbb{Z}_3 \times \mathbb{Z}_5$ o isomorfismo dado

pelo Teorema Chinês do Resto e defina:

$$\begin{array}{rccl} \varphi' : & \mathbb{Z}_{15} & \to & \mathbb{Z}_3 \times \mathbb{Z}_5 \quad \text{com } \varphi(t) = (t_1, t_2). \\ & t & \mapsto & (t_1, 2t_2) \end{array}$$

Vejamos que φ' é um isomorfismo de grupos. De fato, como $\varphi(t) = (t_1, t_2)$, temos $t_1 \equiv t \pmod 3$ e $t_1 \equiv t \pmod 5$. Primeiramente, mostremos que φ' é bem definida. Para tanto, suponha que $t = s$ então $\varphi(t) = (t_1, t_2) = \varphi(s)$ o que implica $\varphi'(t) = (t_1, 2t_2) = \varphi'(s)$ e φ' é bem definida. Agora, vejamos que φ' é injetiva. Para isso, suponha que tenhamos $\varphi'(t) = \varphi'(s)$, então $(t_1, 2t_2) = (s_1, 2s_2)$ se, e somente se, $t_1 = s_1$ e $2t_2 = 2s_2$. Como 2 é invertível módulo 5, resulta que $t_2 = s_1$, e, sendo φ injetiva, temos $t = s$. Também, φ é sobrejetiva, pois dado $(t_1, t_2) \in \mathbb{Z}_3 \times \mathbb{Z}_5$ existe $t \in \mathbb{Z}_{15}$ tal que, $\varphi(t) = (t_1, 3t_2)$, logo $\varphi'(t) = (t_1, 2(3t_2)) = (t_1, t_2)$. Finalmente, vejamos que φ' é homomorfismo, mas isso é claro visto que

$$\varphi'(t) + \varphi'(s) = (t_1, 2t_2) + (s_1, 2s_2) = (t_1 + s_1, 2t_2 + 2s_2) = (t_1 + s_1, 2(t_2 + s_2))$$

com $t_1 \equiv t(mod\ 3)$, $t_2 \equiv t(mod\ 5)$, $s_1 \equiv s \pmod 3$ e $s_2 \equiv s \pmod 5$, assim $t_1 + s_1 \equiv t + s \pmod 3$ e $t_2 + s_2 \equiv t + s \pmod 5$, isto é, $\varphi(t + s) = (t_1 + s_2, t_2 + s_2)$ e, portanto, $(t_1 + s_2, 2(t_2 + s_2)) = \varphi'(t + s)$ e temos $\varphi'(t) + \varphi'(s) = (t_1 + s_2, 2(t_2 + s_2)) = \varphi'(t + s)$.

Como conferimos no Exemplo 2.4.15,

$$\Gamma(\overline{\varphi}(\mathcal{C})) = \{(0,2), (0,3), (0,4), (0,0), (0,1), (1,0), (1,1), (2,0), (2,1)\}$$

é um conjunto de posições de verificação para $\overline{\varphi}(\mathcal{C})$. Assim, usando a Proposição 2.4.19, obtemos

$$(\varphi')^{-1}(\Gamma(\overline{\varphi'}(\mathcal{C})) = (\varphi')^{-1}(\Gamma(\overline{\varphi}(\mathcal{C})) = \{0, 3, 5, 6, 8, 9, 10, 12, 13\} \neq \varphi^{-1}(\Gamma(\overline{\varphi}(\mathcal{C}))$$

um conjunto de posições de verificação para $\mathcal{C}$ distinto do obtido por φ.

Exemplo 2.4.23. Considere o código abeliano $\mathcal{C} \subset \mathbb{F}_2(\mathbb{Z}_5 \times \mathbb{Z}_9)$ dado pelo conjunto definidor:

$$\begin{aligned} \mathcal{D}(\mathcal{C}) = \{&(0,3), (0,6), (1,2), (2,4), (4,8), (3,7), (1,5), (2,1), (4,2), (3,4), (1,8), \\ &(2,7), (4,5), (3,1), (1,6), (2,3), (4,6), (3,3)\} = \mathcal{O}(0,3) \cup \mathcal{O}(1,2) \cup \mathcal{O}(2,3). \end{aligned}$$

Usaremos a construção dada na Observação 2.4.11 para obter um conjunto de posições de verificação para $\mathcal{C}$. Como $\mathcal{D}_1(\mathcal{C}) = \{0, 1, 2, 3, 4, \} = C_5(0) \cup C_5(1)$ podemos tomar

$\overline{D}_1(\mathcal{C}) = \{0, 1\}$ um conjunto completo de representantes de 2-classes ciclotômicas módulo 5 para $\mathcal{D}_1(\mathcal{C}_1)$. Sendo $D_2(0) = \{3, 6\}$, $\gamma_2(0) = 1$ e $6 \in C_9(3)$ temos $\overline{\mathcal{D}}_2(0) = \{0, 3\}$. Também, $\mathcal{D}_1(\mathcal{C})(1) = \{2, 5, 8, 6\}$, $\gamma_2(1) = 4$, $C_{(2^4,9)}(2) = \{2, 5, 8\}$ e $C_{(2^4,9)}(6) = \{6\}$, temos $\overline{\mathcal{D}}_2(1) = \{(1, 2), (1, 6)\}$. Assim,

$$\overline{\mathcal{D}}(\mathcal{C}) = \overline{\mathcal{D}}_2(0) \cup \overline{\mathcal{D}}_2(1) = \{(0, 3), (1, 2), (1, 6)\}$$

Deste modo,

$$M(0) = m(0, 3) = \left|C_{(2,9)}(3)\right| = 2 \text{ e } M(1) = m(1, 2) + m(1, 6) = \left|C_{(2^4,9)}(2)\right| + \left|C_{(2^4,9)}(6)\right| = 4$$

Obtemos, assim

$$f[1] = 4 > f[2] = 2 > f[3] = 0$$

e

$$g[1] = m(1) = 4 < g[2] = m(0) + m(1) = 5$$

Portanto,

$$\begin{aligned}\Gamma(\mathcal{C}) &= \{(i_1, i_2) \in \mathbb{Z}_5 \times \mathbb{Z}_9 : \exists u \in \{1, 2\} \text{ com } f[u + 1] \leq i_2 < f[u] \text{ e } 0 \leq i_1 < g[u]\} \\ &= \{(0, 0), (0, 1), (0, 2), (0, 3), (1, 0), (1, 1), (1, 2), (1, 3), (2, 0), (2, 1), (2, 2), \\ &\quad (2, 3), (3, 0), (3, 1), (3, 2), (3, 3), (4, 0), (4, 1)\}.\end{aligned}$$

O seguinte exemplo mostra que a restrição na escolha de representantes não é supérflua e nos permite evitar redundâncias nas somas.

Exemplo 2.4.24. Considere o código abeliano $\mathcal{C}_1$ com conjunto definidor:

$$\begin{aligned}\mathcal{D}(\mathcal{C}_1) = \{&(0, 3), (0, 6), (1, 2), (2, 4), (4, 8), (3, 7), (1, 5), (2, 1), (4, 2), (3, 4), (1, 8), \\ &(2, 7), (4, 5), (3, 1), (1, 6), (2, 3), (4, 6), (3, 3)\} = \mathcal{O}(0, 3) \cup \mathcal{O}(1, 2) \cup \mathcal{O}(2, 3).\end{aligned}$$

tal como no Exemplo 2.4.23. Note que

$$\overline{D}(\mathcal{C}_1) = \{e^1 = (0, 3), e^2 = (1, 2), e^3 = (2, 3)\}$$

é um conjunto de completo de representantes para $\mathcal{C}_1$, porém este **não** é restrito, isto é, não satisfaz as restrições impostas pela Definição 2.4.10. De fato, note que, por definição, $\gamma_1(e^2)\gamma_1(e^3) = 1$ e temos $C_{(2,5)}(2) = C_{(2,5)}(1)$. Vejamos, que nesse caso, a construção de $\Gamma(\mathcal{C})$ a partir de $\overline{D}(\mathcal{C}_1)$ não tem sentido. Com alguns cálculos, vê-se que

$$m(\pi_1(e^1)) = m(0) = 1,\ m(\pi(e^2)) = m(1) = 4 \text{ e } m(\pi(e^3)) = m(2).$$

Também,

$$m(0,3) = 2,\ m(1,2) = 3 \text{ e } m(2,3) = 1.$$

Assim, $M(0) = 2$, $M(1) = 3$ e $M(2) = 1$ e, portanto, $g[3] = m(0,3)+m(1,2)+m(2,3) = 6$, o que não tem sentido. Porém, trocando-se $e^3 = (2,3)$ por $(1,6)$ tem-se ainda um conjunto de representes que é restrito.

Capítulo 3

Teorema Principal

Neste capítulo provaremos, no Teorema 3.1.8, que $\Gamma(\mathcal{C})$ é um conjunto de posições de verificação para um código $\mathcal{C}$ de $\mathcal{A}(n_1, \ldots, n_\ell)$ arbitrário. Teremos, portanto, que $\Gamma(\mathcal{C})^c$ é um conjunto de informações para $\mathcal{C}$. A prova desse fato está presente em [2, Teorema 9]. Ao fim do Capítulo, na Secção 3.2, daremos algumas aplicações utilizando o conjunto $\Gamma(\mathcal{C})$ para a decodificação de códigos abelianos utilizando o método de decodificação por permutação.

3.1 A prova do Teorema Principal

Seja $\mathcal{C} \subset \mathcal{A}(n_1, \ldots, n_\ell)$ um código abeliano com conjunto definidor $\mathcal{D}(\mathcal{C})$ em relação às n_i-ésimas raízes primitivas da unidade α_i, onde $i = 1, \ldots, \ell$. Suponha $X_1 < \ldots < X_\ell$ e que obtivemos $\overline{\mathcal{D}}(\mathcal{C})$ e $\Gamma(\mathcal{C})$ como nas construções vistas no Capítulo 2, Seção 2.4.

Considere em $\overline{\mathcal{D}}(\mathcal{C})$ uma ordenação qualquer de seus elementos. Para cada $e \in \overline{\mathcal{D}}(\mathcal{C})$ temos a extensão $\mathbb{F}_q \subset \mathbb{F}_{q^{\gamma_{\ell+1}(e)}}$ de grau $\gamma_{\ell+1}(e) = [\mathbb{F}_q^{\gamma_{\ell+1}(e)} : \mathbb{F}_q]$. Além disso, se $e = (e_1, \ldots, e_\ell) \in \overline{\mathcal{D}}(\mathcal{C})$, então

$$[\mathbb{F}_{q^{\gamma_{\ell+1}(e)}} : \mathbb{F}_q] = \gamma_{\ell+1}(e) = mmc(|C_{n_1}(e_1)|, \ldots, |C_{n_\ell}(e_\ell)|).$$

Assim, $m_k := |C_{n_k}(e_k)|$ é um divisor de $\gamma_{\ell+1}(e)$, para cada $k = 1, \ldots, \ell$. Mais ainda, pelo Teorema 1.3.13,

$$m_k = |C_{n_k}(e_k)| = \partial(M_{\alpha^{e_k}})$$

Deste modo, $\mathbb{F}(\alpha^{e_k}) = \mathbb{F}_{q^{m_k}} \subset \mathbb{F}_{q^{\gamma_{\ell+1}(e)}}$, em que $M_{\alpha_k^{e_k}} \in \mathbb{F}_q[X]$ denota o polinômio minimal de $\alpha_k^{e_k}$. Assim, $\mathbb{F}_{q^{\gamma_{\ell+1}(e)}}$ contém as n_k-ésimas raízes da unidade $\alpha_k^{e_k}$ para cada $k = 1, \ldots, \ell$. Em particular, $\alpha_1^{e_1 j_1} \ldots \alpha_\ell^{e_\ell j_\ell} \in \mathbb{F}_{q^{\gamma_{\ell+1}(e)}}$, para cada $\mathbf{j} = (j_1, \ldots, j_\ell) \in \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell}$.

Agora, fixe $\mathscr{B}(e)$ uma $\mathbb{F}_q$-base para o espaço vetorial $\mathbb{F}_{q^{\gamma_{\ell+1}(e)}}$, então existem escalares $\lambda_m = \lambda_m(e) \in \mathbb{F}_q$ tais que

$$\alpha_1^{e_1 j_1} \dots \alpha_\ell^{e_\ell j_\ell} = \sum \lambda_m v_m := h_e^{\mathbf{j}},$$

com $v_m \in \mathscr{B}(e)$ e $1 \leq m \leq \gamma_{\ell+1}(e) = |\mathscr{B}(e)|$. Assim, obtemos para cada $e \in \overline{\mathcal{D}}(\mathcal{C})$ uma expressão, denotada por $h_{\mathbf{j}}^e$, de $\alpha_1^{e_1 j_1} \dots \alpha_\ell^{e_\ell j_\ell}$ em termos de uma base fixada $\mathscr{B}(e)$.

Considere o isomorfismo linear:

$$T : \prod_{e \in \overline{\mathcal{D}}(\mathcal{C})} \mathbb{F}_{q^{\gamma_{\ell+1}(e)}} \to \mathbb{F}_q^{m_0} \tag{3.1}$$

dada pela concatenação dos vetores no produto cartesiano

$$\prod_{e \in \overline{\mathcal{D}}(\mathcal{C})} \mathbb{F}_{q^{\gamma_{\ell+1}(e)}} \text{ e } m_0 = \sum_{e \in \overline{\mathcal{D}}(\mathcal{C})} \gamma_{\ell+1}(e).$$

Note que

$$\sum_{e \in \overline{\mathcal{D}}(\mathcal{C})} \gamma_{\ell+1}(e) = \sum_{e \in \overline{\mathcal{D}}(\mathcal{C})} |\mathcal{O}(e)| = |\mathcal{D}(\mathcal{C})| = |\mathcal{Z}(\mathcal{C})|.$$

Ou seja, $m_0 = |\mathcal{Z}(\mathcal{C})|$. Mais ainda, uma vez que $dim_{\mathbb{F}_q} \mathbb{F}_{q^{|\mathcal{Z}(\mathcal{C})|}} = |\mathcal{Z}(\mathcal{C})|$, temos $\mathbb{F}_{q^{|\mathcal{Z}(\mathcal{C})|}} \simeq \mathbb{F}_q^{|\mathcal{Z}(\mathcal{C})|}$ como $\mathbb{F}_q$-espaços vetoriais. Além disso, para cada $j \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_\ell}$, denotamos por $h_{\mathbf{j}}$ a concatenação dos vetores $h_e^{\mathbf{j}}$ com $e \in \overline{\mathcal{D}}(\mathcal{C})$, isto é, $h_{\mathbf{j}} = (h_e^{\mathbf{j}})_{e \in \overline{\mathcal{D}}(\mathcal{C})}$.

Definição 3.1.1. *Seja $\mathcal{C} \subset \mathcal{A}(n_1, \dots, n_\ell)$ um código abeliano e $\overline{\mathcal{D}}(\mathcal{C})$ um conjunto de representantes restritos para $\mathcal{C}$. Definimos o **tensor verificador** para $\mathcal{C}$ como sendo o conjunto*

$$\mathcal{T}(\mathcal{C}) = \{h_{\boldsymbol{j}} : \boldsymbol{j} \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_\ell}\},$$

em que, $h_{\boldsymbol{j}} = (h_e^{\boldsymbol{j}})_{e \in \overline{\mathcal{D}}(\mathcal{C})}$.

Lema 3.1.2. *Sejam $P(X_1, \dots, X_\ell) = \sum_{\lambda_{j_1, \dots, j_\ell}} X_1^{j_1} \dots X_\ell^{j_\ell} \in \mathcal{A}(n_1, \dots, n_\ell)$, $\mathcal{C}$ um código abeliano sobre $\mathcal{A}(n_1, \dots, n_\ell)$ e $\mathcal{T}(\mathcal{C})$ um tensor verificador para $\mathcal{C}$. Então, uma condição necessária e suficiente para que $P(X_1, \dots, X_\ell) \in \mathcal{C}$ é que $\sum_{\boldsymbol{j}} \lambda_{\boldsymbol{j}} h_{\boldsymbol{j}} = 0 \in \mathbb{F}_{q^{|\mathcal{Z}(\mathcal{C})|}}$.*

Demonstração. Temos

$$P(X_1, \dots, X_\ell) \in \mathcal{C} \iff P(\alpha_1^{e_1}, \dots, \alpha_\ell^{e_\ell}) = 0, \forall (\alpha_1^{e_1}, \dots, \alpha_\ell^{e_\ell}) \in \mathcal{Z}(\mathcal{C}),$$

ou, equivalentemente,

$$P(X_1,\ldots,X_\ell)\in\mathcal{C} \iff P(\alpha_1^{e_1},\ldots,\alpha_\ell^{e_\ell})=0, \forall e=(e_1,\ldots,e_\ell)\in\mathcal{D}(\mathcal{C}).$$

Uma vez que $\overline{\mathcal{D}}(\mathcal{C})$ é, em particular, um conjunto completo de reapresentantes de q-órbitas, uma condição necessária e suficiente para que $P(X_1,\ldots,X_\ell)\in\mathcal{C}$ é que $P(\alpha_1^{e_1},\ldots,\alpha_\ell^{e_\ell})=0$, para cada $e\in\overline{\mathcal{D}}(\mathcal{C})$. Daí, segue

$$\begin{aligned} P(X_1,\ldots,X_\ell)\in\mathcal{C} &\iff P(\alpha_1^{e_1},\ldots,\alpha_\ell^{e_\ell})=0, \forall e\in\overline{\mathcal{D}}(\mathcal{C}) \\ &\iff \sum_{\mathbf{j}=(j_1,\ldots,j_\ell)} \lambda_{j_1,\ldots,j_\ell}\alpha_1^{e_1 j_1}\ldots\alpha_\ell^{e_\ell j_\ell}=0, \forall e\in\overline{\mathcal{D}}(\mathcal{C}). \end{aligned}$$

Note que, cada parcela $\lambda_{j_1,\ldots,j_\ell}\alpha_1^{e_1 j_1}\ldots\alpha_\ell^{e_\ell j_\ell}$, com j variando e e fixo, pertence a $\mathbb{F}_{q^{\gamma_{\ell+1}(e)}}$. Agora, escrevendo $\alpha_1^{e_1 j_1}\ldots\alpha_\ell^{e_\ell j_\ell}=h_e^{\mathbf{j}}$, obtemos que:

$$\sum_{\mathbf{j}}\lambda_{\mathbf{j}}h_e^{\mathbf{j}}=0\in\mathbb{F}_{q^{\gamma_{\ell+1}(e)}}, \forall e\in\overline{\mathcal{D}}(\mathcal{C}) \tag{3.2}$$

Considere T o isomorfismo linear dado em (3.1) e, para fixar as ideias, considere $\overline{\mathcal{D}}(\mathcal{C})=\{e_1,\ldots,e_s\}$ e 3.2, temos

$$\begin{aligned} \sum_{\mathbf{j}}\lambda_{\mathbf{j}}h_{\mathbf{j}} &= \sum_{\mathbf{j}}\lambda_{\mathbf{j}}T(h_{e_1}^{\mathbf{j}},\ldots,h_{e_s}^{\mathbf{j}}) \\ &= \sum_{\mathbf{j}}T(\lambda_{\mathbf{j}}h_{e_1}^{\mathbf{j}},\ldots,\lambda_{\mathbf{j}}h_{e_s}^{\mathbf{j}}) \\ &= T\left(\sum_{\mathbf{j}}\lambda_{\mathbf{j}}h_{e_1}^{\mathbf{j}},\ldots,\sum_{\mathbf{j}}\lambda_{\mathbf{j}}h_{e_s}^{\mathbf{j}})\right) \\ &= T(0,\ldots,0) \\ &= 0\in\mathbb{F}_{q^{|\mathcal{Z}(\mathcal{C})|}}. \end{aligned}$$

Portanto, temos o desejado. □

Lema 3.1.3. *Um conjunto $\mathcal{H}\subset\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_\ell}$ é um conjunto de posições de verificações para um código $\mathcal{C}$ se, e somente se, $\{h_{\mathbf{j}}\}_{\mathbf{j}\in\mathcal{H}}$ é uma base para $\mathcal{T}(\mathcal{C})$, o tensor verificador de $\mathcal{C}$.*

Demonstração. Lembremos que $\mathcal{H}\subset\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_\ell}$ é um conjunto de posições de verificações se, e somente se, as palavras em $\mathcal{C}$ ficam unicamente determinadas por suas entradas em $\mathcal{H}^c$, o complementar de $\mathcal{H}$ em $\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_\ell}$.

Primeiramente, assuma que $\mathcal{H}$ é um conjunto verificador de posições para $\mathcal{C}$ e vejamos que $\{h_{\mathbf{j}}\}_{\mathbf{j}\in\mathcal{H}}$ é base para $\mathcal{T}(\mathcal{C})$. De fato, suponha

$$\sum_{j\in\mathcal{H}} \lambda_{\mathbf{j}} h_{\mathbf{j}} = 0,$$

para convenientes $\lambda_{\mathbf{j}} \in \mathbb{F}_q$. Considere o vetor $c = (c_{\mathbf{j}})_{\mathbf{j}\in\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_\ell}}$ definido por

$$c_{\mathbf{j}} = \begin{cases} 0, \text{ se } j \notin \mathcal{H} \\ c_{\mathbf{j}} = \lambda_{\mathbf{j}}, \text{ se } j \in \mathcal{H}. \end{cases}$$

Como $\sum_{\mathbf{j}} c_{\mathbf{j}} h_{\mathbf{j}} = 0$ segue-se, pelo Lama 3.1.2, que $c \in \mathcal{C}$. Assim, se para algum $\mathbf{j} \in \mathcal{H}$ tivéssemos que $c_{\mathbf{j}} = \lambda_{\mathbf{j}} \neq 0$ então c e a palavras nula seriam elementos distintos de $\mathcal{C}$ que coincidem em $\mathcal{H}^c$, o que é impossível. Logo, $\lambda_{\mathbf{j}} = 0$ para cada $j \in \mathcal{H}$ implicando que $\{h_{\mathbf{j}}\}_{\mathbf{j}\in\mathcal{H}}$ é linearmente independente. Agora, mostremos que $\{h_{\mathbf{j}}\}_{\mathbf{j}\in\mathcal{H}}$ gera $\mathcal{T}(\mathcal{C})$. Para tanto, tome $j_0 \notin \mathcal{H}$, então existem $\{\lambda_{\mathbf{j}}\}_{j\in\mathcal{H}} \subset \mathbb{F}_q$ de modo que $c = (c_{\mathbf{j}})$, definido por

$$c_{\mathbf{j}} = \begin{cases} 0, \text{ se } \mathbf{j} \in \mathcal{H}^c \backslash \{j_0\} \\ 1, \text{ se } \mathbf{j} = \mathbf{j}_0 \\ \lambda_{\mathbf{j}}, \text{ se } j \in \mathcal{H} \end{cases}$$

é uma palavra em $\mathcal{C}$. Deste modo,

$$\begin{aligned} \sum_{\mathbf{j}} c_{\mathbf{j}} h_{\mathbf{j}} = 0 &\iff \sum_{\mathbf{j}\in\mathcal{H}} c_{\mathbf{j}} h_{\mathbf{j}} + \sum_{\mathbf{j}\in\mathcal{H}^c} c_j h_j = 0 \\ &\iff h_{j_0} = \sum_{\mathbf{j}\in\mathcal{H}} (-c_{\mathbf{j}}) h_{\mathbf{j}}, \end{aligned}$$

ou seja, h_{j_0} pertence ao subespaço gerado por $\{h_{\mathbf{j}}\}_{\mathbf{j}\in\mathcal{H}}$ e, portanto, $\{h_{\mathbf{j}}\}_{\mathbf{j}\in\mathcal{H}}$ é base para $\mathcal{T}(\mathcal{C})$.

Reciprocamente, suponha que $\{h_{\mathbf{j}}\}_{\mathbf{j}\in\mathcal{H}}$ seja uma $\mathbb{F}_q$-base para $\mathcal{T}(\mathcal{C})$. Então, para cada $\mathbf{i} \in \mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_\ell}$, $h_{\mathbf{i}}$ é escrito de maneira única como $\mathbb{F}_q$-combinação linear dos elementos de $\{h_{\mathbf{j}}\}_{\mathbf{j}\in\mathcal{H}}$. Tome $c = (c_{\mathbf{j}})$ uma palavra qualquer em $\mathcal{C}$. Pela hipótese, o vetor $\sum_{\mathbf{j}\in\mathcal{H}^c} c_{\mathbf{j}} h_{\mathbf{j}}$ tem expressão única da forma

$$\sum_{\mathbf{j}\in\mathcal{H}^c} c_{\mathbf{j}} h_{\mathbf{j}} = \sum_{\mathbf{j}\in\mathcal{H}} \lambda_{\mathbf{j}} h_{\mathbf{j}},$$

para convenientes $\lambda_{\mathbf{j}} \in \mathbb{F}_q$. Também, como $c \in \mathcal{C}$, vemos

$$\sum_{\mathbf{j}} c_{\mathbf{j}} h_{\mathbf{j}} = 0 = \sum_{\mathbf{j}\in\mathcal{H}^c} c_{\mathbf{j}} h_{\mathbf{j}} - \sum_{\mathbf{j}\in\mathcal{H}} \lambda_{\mathbf{j}} h_{\mathbf{j}} \Rightarrow \sum_{\mathbf{j}\in\mathcal{H}} c_{\mathbf{j}} h_{\mathbf{j}} = -\sum_{\mathbf{j}\in\mathcal{H}} \lambda_{\mathbf{j}} h_{\mathbf{j}}$$
$$\Rightarrow \sum_{\mathbf{j}\in\mathcal{H}} (c_{\mathbf{j}} + \lambda_{\mathbf{j}}) h_{\mathbf{j}} = 0.$$

Daí, sendo $\{h_{\mathbf{j}}\}_{\mathbf{j}\in\mathcal{H}}$ linearmente independente, resulta $c_{\mathbf{j}} = -\lambda_{\mathbf{j}}$, para cada $\mathbf{j} \in \mathcal{H}$. Assim, c fica totalmente determinado por seus valores, $\{c_{\mathbf{j}}\}_{\mathbf{j}\in\mathbb{Z}_{n_1}\times\ldots\times\mathbb{Z}_{n_\ell}}$ uma vez que as escolhas de $\lambda_{\mathbf{j}}$ são únicas a partir das escolhas de $c_{\mathbf{j}}$ com $j \in \mathcal{H}^c$. Assim, $\mathcal{H}^c$ é um conjunto de informações para o código $\mathcal{C}$ e, portanto, $\mathcal{H}$ é um conjunto de posições de verificação para $\mathcal{C}$. □

Lema 3.1.4. *Seja $\mathcal{C} \subset \mathcal{A}(n_1, \ldots, n_\ell)$ um código abeliano, então $|\Gamma(\mathcal{C})| = |\mathcal{Z}(\mathcal{C})|$.*

Demonstração. Para cada $(u_\ell, \ldots, u_2)$ fixado, com $1 \le u_\ell \le s_\ell$ e $1 \le u_i \le s(u_\ell, \ldots, u_{i+1})$, com $2 \le n < \ell$, definimos para $i = 2, \ldots, \ell - 1$:

$$\sigma_i(u_\ell, \ldots, u_{i+1}) = \sum_{u_i=1}^{s(u_\ell,\ldots,u_{i+1})} (f[u_\ell, \ldots, u_{i+1}, u_i] - f[u_\ell, \ldots, u_{i+1}, u_i + 1]) \cdot \ldots \cdot$$
$$\sum_{u_2=1}^{s(u_\ell,\ldots,u_3)} (f[u_\ell, \ldots, u_3, u_2] - f[u_\ell, \ldots, u_3, u_2 + 1]) \cdot g[u_\ell, \ldots, u_3, u_2].$$

Note que

$$\sigma_{i+1}(u_\ell, \ldots, u_{i+2}) = \sum_{u_i=1}^{s(u_\ell,\ldots,u_{i+2})} (f[u_\ell, \ldots, u_{i+1}, u_{i+1}] - f[u_\ell, \ldots, u_{i+1} + 1]) \cdot$$
$$\sum_{u_i=1}^{s(u_\ell,\ldots,u_{i+1})} (f[u_\ell, \ldots, u_{i+1}, u_i] - f[u_\ell, \ldots, u_{i+1}, u_i + 1]) \cdot \ldots \cdot$$
$$\sum_{u_2=1}^{s(u_\ell,\ldots,u_3)} (f[u_\ell, \ldots, u_3, u_2] - f[u_\ell, \ldots, u_3, u_2 + 1]) \cdot g[u_\ell, \ldots, u_3, u_2]$$
$$= \sum_{u_{i+1}=1}^{s(u_\ell,\ldots,u_{i+2})} (f[u_\ell, \ldots, u_{i+1}] - f[u_\ell, \ldots, u_{i+1} + 1]) \sigma_i(u_\ell, \ldots, u_{i+1}). \tag{3.3}$$

Afirmamos que

$$|\Gamma(\mathcal{C})| = \sum_{(u_\ell,\ldots,u_{i+1})} (f[u_\ell] - f[u_\ell + 1]) \cdot \ldots \cdot (f[u_\ell, \ldots, u_{i+1}] - f[u_\ell, \ldots, u_{i+1} + 1]) \sigma_i(u_\ell, \ldots, u_{i+1})$$

para cada $i = 2, \ldots, \ell - 1$. Provemos a afirmação por indução sobre $i \geq 2$. Com efeito, para $i = 2$ vemos, pela Proposição 2.4.12,

$$\begin{aligned}
|\Gamma(\mathcal{C})| &= \sum_{(u_\ell,\ldots,u_2)} (f[u_\ell] - f[u_\ell + 1]) \cdot \ldots \cdot (f[u_\ell, \ldots, u_2] - f[u_\ell, \ldots, u_2 + 1])(g[u_\ell, \ldots, u_2]) \\
&= \sum_{(u_\ell,\ldots,u_3)} \Bigg((f[u_\ell] - f[u_\ell + 1]) \cdot \ldots \cdot (f[u_\ell, \ldots, u_3] - f[u_\ell, \ldots, u_3 + 1]) \\
&\quad \cdot \sum_{u_2=1}^{s(u_\ell,\ldots,u_3)} (f[u_\ell, \ldots, u_3, u_2] - f[u_\ell, \ldots, u_3, u_2 + 1])g[u_\ell, \ldots, u_2]) \Bigg) \\
&= \sum_{(u_\ell,\ldots,u_3)} (f[u_\ell] - f[u_\ell + 1]) \cdot \ldots \cdot (f[u_\ell, \ldots, u_3] - f[u_\ell, \ldots, u_3 + 1])\sigma_2(u_\ell, \ldots, u_3).
\end{aligned}$$

e temos os passo indutivo. Agora, suponha que a afirmação seja valida para $i \geq 2$ e certifiquemos que vale para $i + 1$. De fato,

$$\sum_{(u_\ell,\ldots,u_{i+2})} (f[u_\ell] - f[u_\ell + 1]) \cdot \ldots \cdot (f[u_\ell, \ldots, u_{i+2}] - f[u_\ell, \ldots, u_{i+2} + 1])\sigma_{i+1}(u_\ell, \ldots, u_{i+2})$$

Logo, substituindo a expressão σ_{i+1}, como em (3.3), na equação anterior, temos

$$\begin{aligned}
&\sum_{(u_\ell,\ldots,u_{i+2})} \Big[\big((f[u_\ell] - f[u_\ell + 1]) \cdot \ldots \cdot (f[u_\ell, \ldots, u_{i+2}] - f[u_\ell, \ldots, u_{i+2} + 1]) \big) \\
&\cdot \sum_{u_{i+1}}^{s(u_\ell,\ldots,u_{i+2})} (f[u_\ell, \ldots, u_{i+1}] - f[u_\ell, \ldots, u_{i+1} + 1])\sigma_i(u_\ell, \ldots, u_{i+1}) \Big] \\
= &\sum_{(u_\ell,\ldots,u_{i+1})} (f[u_\ell] - f[u_\ell + 1]) \cdot \ldots \cdot (f[u_\ell, \ldots, u_{i+1}] - f[u_\ell, \ldots, u_{i+1} + 1])\sigma_i(u_\ell, \ldots, u_{i+1}).
\end{aligned}$$

Assim, a afirmação fica provada. Em particular,

$$|\Gamma(\mathcal{C})| = \sum_{u_\ell=1}^{s_\ell} (f[u_\ell] - f[u_\ell + 1])\sigma_{\ell-1}(u_\ell). \tag{3.4}$$

Além disso, para cada $i = 2, \ldots, \ell - 1$, vale que:

$$\sigma_i(u_\ell, \ldots, u_{i+1}) = \sum_{e \in \overline{D}_{i-1}(C)} \mu_{u_\ell,\ldots,u_{i+1}} \cdot \gamma_i(e). \tag{3.5}$$

Mostremos a igualdade em (3.5) por indução sobre i. Para $i = 2$, temos:

$$\sigma_2(u_\ell, \ldots, u_3) = \sum_{u_2=1}^{s(u_\ell,\ldots,u_3)} (f[u_\ell, \ldots, u_3, u_2] - f[u_\ell, \ldots, u_3, u_2 + 1])g[u_\ell, \ldots, u_2] \tag{3.6}$$

Temos

$$g[u_\ell, \ldots, u_2] = \sum_{\substack{e \in \overline{D}_1(\mathcal{C}) \\ \mu_{u_\ell,\ldots,u_3} \geq f[u_\ell,\ldots,u_2]}} m(e) \tag{3.7}$$

Daí, substituindo (3.7) em (3.6), segue

$$\sigma_2(u_\ell,\ldots,u_3)=\sum_{u_2=1}^{s(u_\ell,\ldots,u_3)}(f[u_\ell,\ldots u_3,u_2]-f[u_\ell,\ldots,u_3,u_2+1])\cdot\sum_{\substack{e\in\overline{D}_1(\mathcal{C})\\ \mu_{u_\ell,\ldots,u_3}(e)\geq f[u_\ell,\ldots,u_2]}}m(e). \tag{3.8}$$

Por outro lado, dado $e\in\overline{D}_1$, segue, $\mu_{u_\ell,\ldots,u_3}(e)\geq f[u_\ell,\ldots,u_3,t]$, para algum $1\leq t\leq s(u_\ell,\ldots,u_2)$. Reciprocamente, dado $1\leq u_2\leq s(u_\ell,\ldots,u_3)$, deve existir $e\in\overline{D}_1(\mathcal{C})$ tal que $\mu_{u_\ell,\ldots,u_3}(e)\geq f[u_\ell,\ldots,u_3,u_2]$. Desse modo, podemos fatorar $m(e)$ expressão (3.8) e obter:

$$\sigma_2(u_\ell,\ldots,u_3)=\sum_{e\in\overline{D}_1(\mathcal{C})}\left[m(e)\cdot\sum_{f[u_\ell,\ldots,u_2]\leq\mu_{u_\ell,\ldots,u_3}(e)}(f[u_\ell,\ldots,u_2]-f[u_\ell,\ldots,u_2+1])\right]. \tag{3.9}$$

Além disso, existe $1\leq t=t(e)\leq s(u_\ell,\ldots,u_3)$ tal que, $f[u_\ell,\ldots,u_3,t]=\mu_{u_\ell,\ldots,u_3}(e)$. Ainda se $k<t<j$ então:

$$f[u_\ell,\ldots,u_3,j]<f[u_\ell,\ldots,u_3,t]=\mu_{u_\ell,\ldots,u_3}(e)<f[u_\ell,\ldots,u_3,k].$$

Dessa maneira,

$$\begin{aligned}
&\sum_{f[u_\ell,\ldots,u_2]\leq\mu_{u_\ell,\ldots,u_3}(e)}f[u_\ell,\ldots,u_2]-f[u_\ell,\ldots,u_2+1]\\
=\;& f[u_\ell,\ldots,u_3,t]-f[u_\ell,\ldots,u_3,t+1]\\
+\;& f[u_\ell,\ldots,u_3,t+1]-f[u_\ell,\ldots,u_3,t+2]\\
\ldots\;&\\
+\;& f[u_\ell,\ldots,u_3,s(u_\ell,\ldots,u_2)-1]-f[u_\ell,\ldots,u_3,s(u_\ell,\ldots,u_2)]\\
+\;& f[u_\ell,\ldots,u_3,s(u_\ell,\ldots,u_2)]-f[u_\ell,\ldots,u_3,s(u_\ell,\ldots,u_2)+1]\\
=\;& f[u_\ell,\ldots,u_3,t]\\
=\;& \mu_{u_\ell,\ldots,u_3}(e),
\end{aligned} \tag{3.10}$$

pois $f[u_\ell,\ldots,u_3,s(u_\ell,\ldots,u_2)+1]=0$. Substituindo (3.10) em (3.9), obtemos:

$$\sigma_2(u_\ell,\ldots,u_3)=\sum_{e\in\overline{D}_1(\mathcal{C})}m(e)\mu_{u_\ell,\ldots,u_3}(e)=\sum_{e\in\overline{D}_1(\mathcal{C})}\gamma_2(e)\mu_{u_\ell,\ldots,u_3}(e)$$

e temos o passo indutivo. Suponha

$$\sigma_i(u_\ell,\ldots,u_{i+1})=\sum_{e\in\overline{D}_{i-1}(\mathcal{C})}\mu_{u_\ell,\ldots,u_{i+1}}(e).\gamma_i(e),$$

para algum $2 \leq i < l-1$ e vejamos que a igualdade se verifica para $i+1$. De fato, temos, por (3.3),

$$\sigma_{i+1}(u_\ell, \ldots, u_{i+2}) = \sum_{u_{i+1}=1}^{s(u_\ell,\ldots,u_{i+2})} (f[u_\ell, \ldots, u_{i+1}] - f[u_\ell, \ldots, u_{i+1}+1]) \cdot \sigma_i(u_\ell, \ldots, u_{i+1})$$

Logo, pela hipótese de indução,

$$\begin{aligned}\sigma_{i+1}(u_\ell, \ldots, u_{i+2}) = & \sum_{u_{i+1}=1}^{s(u_\ell,\ldots,u_{i+2})} (f[u_\ell, \ldots, u_{i+1}] - f[u_\ell, \ldots, u_{i+1}+1]) \\ & \cdot \sum_{e \in \overline{D}_{i-1}(\mathcal{C})} \mu_{u_\ell,\ldots,u_{i+1}}(e).\gamma_i(e)\end{aligned}$$

Assim, substituindo

$$\mu_{u_\ell,\ldots,u_{i+1}}(e) = \sum_{\mu_{u_\ell,\ldots,u_{i+2}}(e,a) \geq f[u_\ell,\ldots,u_{i+1}]} m(e,a)$$

na igualdade anterior, obtemos

$$\begin{aligned}\sigma_{i+1}(u_\ell, \ldots, u_{i+2}) \quad = \quad & \sum_{u_{i+1}=1}^{s(u_\ell,\ldots,u_{i+2})} (f[u_\ell, \ldots, u_{i+1}] - f[u_\ell, \ldots, u_{i+1}+1]) \cdot \\ & \sum_{e \in \overline{D}_{i-1}(\mathcal{C})} \gamma_i(e) \cdot \left(\sum_{\mu_{u_\ell,\ldots,u_{i+2}}(e,a) \geq f[u_\ell,\ldots,u_{i+1}]} m(e,a) \right) \qquad (3.11)\end{aligned}$$

Também, veja (2.1),

$$\sum_{\mu_{u_\ell,\ldots,u_{i+2}}(e,a) \geq f[u_\ell,\ldots,u_{i+1}]} \gamma_i(e) m(e,a) = \sum_{\mu_{u_\ell,\ldots,u_{i+2}}(e,a) \geq f[u_\ell,\ldots,u_{i+1}]} \gamma_{i+1}(e,a). \qquad (3.12)$$

Agora, dado $e = (e_1, \ldots, e_i) \in \overline{D}_i(\mathcal{C})$, $\mu_{u_\ell,\ldots,u_{i+2}}(e) = f[u_\ell, \ldots, u_{i+2}, t]$ para algum $1 \leq t \leq s(u_\ell, \ldots, u_{i+2})$, uma vez que $\pi_{i-1}(e) \in \overline{D}_{i-1}(\mathcal{C})$. Além disso, e_i satisfaz

$$\mu_{u_\ell,\ldots,u_{i+2}}(e_1, \ldots, e_{i-1}, e_i) \geq f[u_\ell, \ldots, u_{i+2}, u_{i+1}]$$

para cada $u_{i+1} \geq t$. Por outro lado, dado $e \in \overline{D}_{i-1}(\mathcal{C})$ e $a \in R(e)$, deve existir u_{i+1} tal que

$$\mu_{u_\ell,\ldots,u_{i+2}}(e,a) \geq f[u_\ell, \ldots, u_{i+2}, u_{i+1}].$$

Com a finalidade de facilitar a notação, considere $\mu(e) = \mu_{u_\ell,\ldots,u_{i+2}}(e)$. Pelo que acabamos de argumentar, e por (3.12),

$$\sum_{e \in \overline{D}_{i-1}(\mathcal{C})} \gamma_i(e) \cdot \left(\sum_{\mu_{u_\ell,\ldots,u_{i+2}}(e,a) \geq f[u_\ell,\ldots,u_{i+1}]} m(e,a) \right) = \sum_{e \in \overline{D}_i(\mathcal{C})} \gamma_{i+1}(e). \qquad (3.13)$$

Assim, substituindo (3.12) em (3.11), obtemos:

$$\begin{aligned}\sigma_{i+1}(u_\ell,\ldots,u_{i+2}) &= \sum_{e\in\overline{D}_i(\mathcal{C})}\gamma_{i+1}(e)\cdot\sum_{f[u_\ell,\ldots,u_{i+1}]\leq\mu(e)}(f[u_\ell,\ldots,u_{i+1}]-f[u_\ell,\ldots,u_{i+1}+1])\\ &= \sum_{e\in\overline{D}_i(\mathcal{C})}\gamma_{i+1}(e)\mu(e).\end{aligned}$$

Assim, pelo princípio indução, o resultado fica estabelecido. Em particular,

$$\begin{aligned}|\Gamma(\mathcal{C})| &= \sum_{u_\ell=1}^{s_\ell}(f[u_\ell]-f[u_\ell+1])\cdot\sigma_{\ell-1}(u_\ell)\ \text{(por (3.4))}\\ &= \sum_{u_\ell=1}^{s_\ell}(f[u_\ell]-f[u_\ell+1])\cdot\sum_{e\in\overline{D}_{\ell-2}}\gamma_{l-1}(e)\cdot\mu_{u_\ell}(e)\\ &= \sum_{u_\ell}^{s_\ell}(f[u_\ell]-f[u_\ell+1])\cdot\sum_{e\in\overline{D}_{\ell-2}}\gamma_{l-1}(e)\left(\sum_{M(e,a)\geq f[u_\ell]}m(e,a)\right)\\ &= \sum_{e\in\overline{D}_{\ell-1}}\gamma_\ell(e)\cdot\sum_{f[u_\ell]\leq M(e)}(f[u_\ell]-f[u_\ell+1])\\ &= \sum_{e\in\overline{D}_{\ell-1}(\mathcal{C})}\gamma_\ell(e)M(e)\\ &= \sum_{e\in\overline{D}_{\ell-1}(\mathcal{C})}\gamma_\ell(e)\left(\sum_{a\in R(e)}m(e,a)\right)\ \text{(veja (2.2))}\\ &= \sum_{e\in\overline{\mathcal{D}}(\mathcal{C})}\gamma_{\ell+1}(e).\end{aligned}$$

Finalmente, como $e\in\overline{\mathcal{D}}(\mathcal{C})$ e este é um conjunto completo de representantes de órbitas para $\mathcal{C}$, o resultado segue pela Proposição 2.4.7. □

Estamos quase prontos para demonstrar o teorema principal deste estudo. Introduziremos alguns conceitos e notações para, em seguida, enunciar o teorema.

Definição 3.1.5. *Considere $u=(u_\ell,\ldots,u_2)$ uma sequência obtida na construção de $\Gamma(\mathcal{C})$. Podemos considerar o conjunto:*

$$\Upsilon := \{(u_\ell,\ldots,u_2) : 1\leq u_\ell\leq s_\ell \text{ e } 1\leq u_i\leq s(u_\ell,\ldots,u_{i+1}),\ \text{para } 1\leq i\leq\ell-1\}\subset\mathbb{N}^{\ell-2}.$$

Dessa forma, podemos munir Υ da ordem lexicográfica usual. Isto é, dados $u=(u_\ell,\ldots,u_2)$, $u'=(u'_\ell,\ldots,u'_2)\in\Upsilon$, definimos que $u\leq u'$ se, e somente se, $u_\ell\leq u'_\ell$ ou $u_j=u'_j$ para $j=\ell,\ldots,i+1\geq 2$ e $u_i\leq u'_i$.

Definição 3.1.6. *Dado um elemento* $\boldsymbol{j} = (j_1, \ldots, j_\ell) \in \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell}$ *temos que* $\boldsymbol{j} \in \Gamma(\mathcal{C})$ *se, e somente se, existe* $(u_\ell, \ldots, u_2) \in \Upsilon$*, tal que* $f[u_\ell, \ldots, u_i + 1] \leq j_i < f[u_\ell, \ldots, u_i]$ *para cada* $i = 2, \ldots, \ell$ *e* $1 \leq j_1 \leq g[u_\ell, \ldots, u_2]$*. Definimos* $\overline{u}_{\boldsymbol{j}} := (u_\ell, ..., u_2)$ *como sendo elemento* $u \in \Upsilon$ *de modo que* $\boldsymbol{j}$ *é obtido das restrições* u*.*

Observação 3.1.7. Note que a definição anterior está bem posta, pois, pela demonstração da Proposição 2.4.12, para cada $\mathbf{j} \in \Gamma(\mathcal{C})$, existe um único $u \in \Upsilon$ de modo que j é obtido a partir das restrições u.

Teorema 3.1.8. *Seja* $\mathcal{C} \subset \mathcal{A}(n_1, \ldots, n_\ell)$ *um código abeliano com conjunto definidor* $\mathcal{D}(\mathcal{C})$*. Então,* $\Gamma(\mathcal{C})$ *é um conjunto de posições de verificação para* $\mathcal{C}$*.*

Demonstração. Pelo Lema 3.1.3, basta provar que o conjunto $\{h_{\mathbf{j}}\}_{\mathbf{j}\in\Gamma(\mathcal{C})}$ é base para o $\mathbb{F}_q$-subespaço vetorial gerado pelo tensor verificador $\mathcal{T}(\mathcal{C})$. Como, devido ao Lema 3.1.4, $|\Gamma(\mathcal{C})| = |\mathcal{Z}(\mathcal{C})|$ é necessário e suficiente ver que o conjunto $\{h_{\mathbf{j}}\}_{\mathbf{j}\in\Gamma(\mathcal{C})}$ é linearmente independente, pois $\langle\mathcal{T}(\mathcal{C})\rangle \subset \mathbb{F}_{q^{|\mathcal{Z}(\mathcal{C})|}}$ e a dimensão de $\mathbb{F}_{q^{|\mathcal{Z}(\mathcal{C})|}}$ sobre $\mathbb{F}_q$ é $|\mathcal{Z}(\mathcal{C})|$. Para tanto, considere uma família $\{\lambda_{\mathbf{j}}\}_{\mathbf{j}\in\Gamma(\mathcal{C})}$ de coeficientes em $\mathbb{F}_q$ não todos nulos. Mostraremos que $\sum_{\mathbf{j}\in\Gamma(\mathcal{C})} \lambda_{\mathbf{j}} h_{\mathbf{j}} \neq 0$ o que concluirá a demonstração. Vamos provar que existe $(e_1, ..., e_\ell) \in \overline{\mathcal{D}}(\mathcal{C})$ tal que,

$$\sum_{\mathbf{j}=(j_1,\ldots,j_\ell)\in\Gamma(\mathcal{C})} \lambda_{\mathbf{j}} \alpha_1^{e_1 j_1} \cdot \ldots \cdot \alpha_\ell^{e_\ell j_\ell} \neq 0. \tag{3.14}$$

Para ver isso, fixe $\mathbf{i} = (i_1, ..., i_\ell) \in \Gamma(\mathcal{C})$ tal que $\overline{u}_{\mathbf{i}} = min\{\overline{u}_{\mathbf{j}} \in \Upsilon : \lambda_{\mathbf{j}} \neq 0\}$. Defina $\overline{v}_{\mathbf{i}} = (v_\ell, ..., v_2) = \overline{u}_{\mathbf{i}}$. Construiremos, de maneira indutiva, um elemento $(e_1, .., e_\ell) \in \overline{\mathcal{D}}(\mathcal{C})$ tal que para cada $k = 1, .., \ell$

$$\sum_{\mathbf{j}=(j_1,\ldots,j_k,i_{k+1},\ldots,i_\ell)\in\Gamma(\mathcal{C})} \lambda_{\mathbf{j}} \alpha_1^{e_1 j_1} \cdot \ldots \cdot \alpha_k^{e_k j_k} \neq 0 \tag{3.15}$$

e enquanto $k < \ell$,

$$\mu_{v_\ell,\ldots,v_{k+2}}(e_1, \ldots, e_k) \geq f[v_\ell, ..., v_{k+1}] \text{ se } k < \ell - 2 \tag{3.16}$$

$$M(e_1, \ldots, e_{\ell-1}) \geq f[v_\ell] \text{ se } k = \ell - 1. \tag{3.17}$$

Começamos com $k = 1$. Pela definição de $\overline{v}_{\mathbf{i}}$ e uma vez que $\mathbf{i} \in \Gamma(\mathcal{C})$, temos $1 \leq i_1 < g[v_\ell, \ldots, v_2]$. Considere o polinômio

$$P(X_1) = \sum_{\mathbf{j}=(j_1,i_2,\ldots,i_\ell)\in\Gamma(\mathcal{C})} \lambda_{\mathbf{j}} X_1^{j_1}.$$

Assim, pela definição de $\Gamma(\mathcal{C})$, $\overline{u}_{\mathbf{j}} = \overline{u}_{\mathbf{i}}$, para $\mathbf{j} = (j_1, i_2, \ldots, i_\ell)$, então j_1 deve satisfazer $1 \leq j_1 < g[v_\ell, \ldots, v_2]$ e temos $(j_1, i_2, \ldots, i_\ell) \in \Gamma(\mathcal{C})$. Assim,

$$\delta := gr(P(X_1)) \leq max\{j_1 : 1 \leq j_1 < g[v_\ell, \ldots, v_2]\} < g[v_\ell, \ldots, v_2] \tag{3.18}$$

Também

$$\begin{aligned} g[v_\ell, \ldots, v_2] &= \sum_{\substack{e \in \overline{D}_1(\mathcal{C}) \\ \mu_{v_\ell, \ldots, v_3}(e) \geq f[v_\ell, \ldots, v_2]}} m(e) \\ &= \sum_{\substack{e \in \overline{D}_1(\mathcal{C}) \\ \mu_{v_\ell, \ldots, v_3}(e) \geq f[v_\ell, \ldots, v_2]}} |C_{(q,n_1)}(e)| \\ &= \left| \bigcup \{C_{(q,n_1)}(e) : e \in \overline{D}_1(\mathcal{C}), \mu_{v_\ell, \ldots, v_3}(e) \geq f[v_\ell, \ldots, v_2]\} \right|. \end{aligned}$$

Uma vez que $\overline{D}_1(\mathcal{C})$ é um conjunto completo de q-classes ciclotômicas para $\pi_1(\mathcal{C})$, na verdade, temos

$$g[v_\ell, \ldots, v_2] = \left| \bigcup \{C_{(q,n_1)}(e) : e \in \overline{D}_1(\mathcal{C}), \mu_{v_\ell, \ldots, v_3}(e) \geq f[v_\ell, \ldots, v_2]\} \right|.$$

Como $P(X_1) \in \mathbb{F}_q[X_1]$, deve existir $e_1 \in \overline{D}_1(\mathcal{C})$ satisfazendo (3.16) e, além disso, $P(\alpha_1^{e_1}) \neq 0$. De fato, se $P(\alpha_1^{e_1}) = 0$ para cada $e_1 \in \overline{D}_1(\mathcal{C})$ com $\mu_{v_\ell, \ldots, v_3}(e_1) \geq f[v_\ell, \ldots, v_2]$, então

$$P(\alpha_1^{e_1 j_1}) = 0, \forall j_1 \in C_{(q,n_1)}(e_1)$$

implicando

$$(X_1 - \alpha_1^{e_1 j_1}) \mid P(X), \forall j_1 \in C_{(q,n_1)}(e_1).$$

Logo, isso valendo para cada $e_1 \in \overline{D}_1(\mathcal{C})$, temos

$$\delta \geq \sum_{\substack{e \in \overline{D}_1(\mathcal{C}) \\ \mu_{v_\ell, \ldots, v_3}(e) \geq f[v_\ell, \ldots, v_3]}} gr(X_1 - \alpha_1^{e_1 j_1}) = g[v_\ell, \ldots, v_2],$$

o que contradiz (3.18). Isso prova o passo indutivo. Suponha que tenhamos construído $e = (e_1, ..., e_k) \in \overline{D}_k(\mathcal{C})$ satisfazendo (3.15) e (3.16). Daremos o passo $k+1$. Considere o polinômio

$$P_e(X_{k+1}) = \sum_{\mathbf{j} = (j_1, \ldots, j_{k+1}, i_{k+2}, \ldots, i_\ell) \in \Gamma(\mathcal{C})} \lambda_{\mathbf{j}} \alpha_1^{e_1 j_1} \cdot \ldots \cdot \alpha_k^{e_k j_k} X_{k+1}^{j_k + 1}.$$

Então, para qualquer $\mathbf{j} = (j_1, \ldots, j_{k+1}, i_{k+2}, \ldots, i_\ell) \in \Gamma(\mathcal{C})$ nos temos, sempre que $\lambda_\mathbf{j} \neq 0$, que $\overline{u}_\mathbf{j} = (u_\ell, \ldots, u_2)$ satisfaz $u_\ell = v_\ell, \ldots, u_{k+2} = v_{k+2}$. Também, pela definição de $\overline{v}_\mathbf{i}$, $\overline{u}_\mathbf{j} \geq \overline{v}_\mathbf{i}$, implicando

$$f[v_\ell, \ldots, u_{k+1} + 1] \leq j_{\ell+1} < f[v_\ell, \ldots, u_{k+1}] \leq f[v_\ell, \ldots, v_{k+1}].$$

Logo, $gr(P_e(X_{k+}) < f[v_\ell, \ldots, u_k]$ e, pela hipótese de indução, temos

$$\mu_{v_\ell, \ldots, v_{k+2}}(e) \geq f[v_\ell, \ldots, v_{k+1}].$$

Como no caso $\ell = 1$, uma vez que $\overline{\mathcal{D}}(\mathcal{C})$ é um conjunto restrito de representantes, segue

$$\mu_{v_\ell, \ldots, v_{k+2}}(e) = \left| \bigcup \{ C_{(q^{\gamma_{k+1}(e)}, r_{k+1}}(a) : (e, a) \in \overline{D}_{k+1}(\mathcal{C}), \mu_{v_\ell, \ldots, v_{k+2}}(e) \geq f[v_\ell, \ldots, v_{k+1}] \} \right|$$

Dessa maneira, como $P_e(X_{\ell+1}) \in \mathbb{F}_{q^{\gamma_{\ell+1}(e)}}[X_{k+1}]$, deve existir $e_{k+1} \in \mathbb{Z}_{r_{k+1}}$ satisfazendo (3.15) e (3.16). Agora, podemos dar o passo $k = \ell - 1$ e de forma análoga obter (3.17). Agora, suponha que exista $e = (e_1, \ldots, e_{\ell-1}) \in \overline{D}_{\ell-1}$ satisfazendo (3.15), (3.16) e (3.17). Considere o polinômio

$$P_e(X_\ell) = \sum_{\mathbf{j}=(j_1, \ldots, j_\ell)} \lambda_\mathbf{j} \alpha_1^{e_1 j_1} \cdot \ldots \cdot \alpha_{\ell-1}^{e_{\ell-1} j_{\ell-1}} \cdot X_\ell^{j_\ell}.$$

Do mesmo modo, se $\lambda_\mathbf{j} \neq 0$ então $\overline{u}_\mathbf{j} \geq \overline{v}_\mathbf{i}$ implicando $u_\ell \geq v_\ell$. Com isso em mente, $f[u_\ell] \leq f[v_\ell]$, $gr(P_e(X_\ell)) < f[v_\ell] \leq M(e) = \sum_{a \in R(e)} m(e, a)$. Assim, existe $e_\ell \in \mathbb{Z}_{r_\ell}$ tal que $(e_1, \ldots, e_\ell) \in \overline{\mathcal{D}}(\mathcal{C})$, com

$$P_e(\alpha_\ell^{e_\ell}) = \sum_{\mathbf{j}=(j_1, \ldots, j_\ell) \in \Gamma(\mathcal{C})} \lambda_\mathbf{j} \alpha_1^{e_1 j_1} \cdot \ldots \cdot \alpha_\ell^{e_\ell j_\ell} \neq 0. \tag{3.19}$$

Finalmente, considere

$$\sum_{\mathbf{j} \in \Gamma(\mathcal{C})} \lambda_\mathbf{j} h_\mathbf{j}; \{0\} \neq \{\lambda_\mathbf{j}\}_{\mathbf{j} \in \Gamma(\mathcal{C})} \subset \mathbb{F}_q.$$

Pelo que acabamos de ver, existe ao menos um $e \in \overline{\mathcal{D}}(\mathcal{C})$ tal que (3.14) se verifica. Sem perda de generalidade, fixe $\overline{\mathcal{D}}(\mathcal{C}) = \{e^1, \ldots, e^k\}$. Considere T o isomorfismo como em (3.1), então $\lambda_\mathbf{j} h_\mathbf{j} = \lambda_\mathbf{j} T(h_{e^i}^\mathbf{j}) = T(\lambda_\mathbf{j} h_{e^i}^\mathbf{j})$ com $i = 1, \ldots, k$. Logo,

$$\begin{aligned}
\sum_{\mathbf{j} \in \Gamma(\mathcal{C})} \lambda_\mathbf{j} h_\mathbf{j} &= \sum_{\mathbf{j} \in \Gamma(\mathcal{C})} T(\lambda_\mathbf{j} h_{e^1}^\mathbf{j}, \ldots, \lambda_\mathbf{j} h_{e^k}^\mathbf{j}) \\
&= T\left(\sum_{\mathbf{j} \in \Gamma(\mathcal{C})} (\lambda_\mathbf{j} h_{e^1}^\mathbf{j}, \ldots, \lambda_\mathbf{j} h_{e^k}^\mathbf{j}) \right) \\
&= T\left(\sum_{\mathbf{j} \in \Gamma(\mathcal{C})} \lambda_\mathbf{j} h_{e^1}^\mathbf{j}, \ldots, \sum_{\mathbf{j} \in \Gamma(\mathcal{C})} \lambda_\mathbf{j} h_{e^k}^\mathbf{j} \right) \neq 0,
\end{aligned}$$

pois, por (3.14), existe i, tal que:

$$\sum_{\mathbf{j}\in\Gamma(\mathcal{C})} \lambda_{\mathbf{j}} h_{e^i}^{\mathbf{j}} \neq 0.$$

□

Como corolário imediato, temos:

Corolário 3.1.9. *Seja $\mathcal{C}$ um código abeliano sobre $\mathcal{A}(n_1,\ldots,n_\ell)$, então a dimensão de $\mathcal{C}$ sobre $\mathbb{F}_q$ é $k = n - |\mathcal{Z}(\mathcal{C})| = n - |\Gamma(\mathcal{C})|$.*

3.2 Aplicações em decodificação por permutação

Nessa seção mostraremos como o conjunto $\Gamma(\mathcal{C})$ pode ser útil para a decodificação por permutação para códigos abelianos. Na Secção 1.2 apresentamos o algoritmo de decodificação por permutação para códigos lineares em $\mathbb{F}^n$. A seguir exibiremos como esse conceito se relaciona no contexto de códigos abelianos em $\mathcal{A}(n_1,\ldots,n_\ell)$.

Denotamos por $S_{n_1\times\ldots\times n_\ell}$ o conjunto de todas as permutações de $G := \mathbb{Z}_{n_1}\times\ldots\times\mathbb{Z}_{n_\ell}$. Para cada $\sigma \in S_{n_1\times\ldots\times n_\ell}$, podemos considerar o automorfismo linear

$$\begin{array}{rccc} \overline{\sigma}: & \mathcal{A}(n_1,\ldots,n_\ell) & \to & \mathcal{A}(n_1,\ldots,n_\ell) \\ & \sum_{j\in G} a_j X^j & \mapsto & \sum_{j\in G} a_{\sigma^{-1}(j)} X^j \end{array}.$$

que extende σ, isto é, $\overline{\sigma}|_G = \sigma$. Além disso, por simplicidade, denotamos $\overline{\sigma} = \sigma$ e dizemos que σ é um **automorfismo de permutação** sobre $\mathcal{A}(n_1,\ldots,n_\ell)$.

Observação 3.2.1. Note que, como $\mathcal{A}(n_1,\ldots,n_\ell) \simeq \mathbb{F}G$ e $G \subset \mathbb{F}G$ podemos considerar $G \subset \mathcal{A}(n_1,\ldots,n_\ell)$. Além disso, dado $\sigma \in S_{n_1\times\ldots\times n_\ell}$, definir um automorfismo de permutação em $\mathcal{A}(n_1,\ldots,n_\ell)$, equivale a definir o $\mathbb{F}$-automorfismo linear,

$$\begin{array}{rccc} \sigma: & \mathbb{F}G & \to & \mathbb{F}G \\ & \sum_{g\in G} a_g g & \mapsto & \sum_{g\in G} a_{\sigma^{-1}(g)} g \end{array} \tag{3.20}$$

Perceba que, a rigor, deveríamos definir σ como $\sigma(\sum a_g g) = \sum a_g \sigma(g)$, visto que G é uma base para $\mathbb{F}G$. Entretanto, se $\sigma(\sum a_g g) = \sum a_g \sigma(g)$, então o coeficiente de $g \in G$, após a ação de σ, é $\sigma^{-1}(g)$ e, portanto, a definição de σ, em (3.20), fica bem posta.

Assim, nesse contexto, temos:

Definição 3.2.2. *Seja $\mathcal{C} \subset \mathcal{A}(n_1, \ldots, n_\ell)$ um código abeliano, definimos o* ***grupo dos automorfismos de permutação*** *de $\mathcal{C}$ como sendo* $\mathrm{PAut}(\mathcal{C}) = \{\sigma \in G : \sigma(\mathcal{C}) = \mathcal{C}\}$.

Vejamos alguns exemplos de automorfismos de permutação.

Exemplo 3.2.3. Considere o automorfismo linear sobre $\mathcal{A}(n_1, \ldots, n_\ell)$, definido por

$$\sigma_s(p(X_1, \ldots, X_\ell) = X_s \cdot p(X_1, \ldots, X_\ell)$$

para cada $s = 1, \ldots, \ell$. Note que σ_s é um automorfismo de permutação induzido pela permutação $\sigma_s \in S_{n_1 \times \ldots \times n_\ell}$, dada por

$$\sigma(i_1, \ldots, i_\ell) = (i_1, \ldots, i_s + 1, \ldots, i_\ell).$$

Também, para todo código abeliano $\mathcal{C} \subset \mathcal{A}(n_1, \ldots, n_\ell)$, tem-se $\sigma_s \in \mathrm{PAut}(\mathcal{C})$. De fato, como $\mathcal{C}$ é um ideal, para cada $c = c(X_1, \ldots, X_\ell) \in \mathcal{C}$, temos $X_s \cdot c \in \mathcal{C}$. Logo, $\sigma_s(\mathcal{C}) \subset \mathcal{C}$. Ainda, como $\sigma_s(\mathcal{C})$ e $\mathcal{C}$ possuem a mesma dimensão como $\mathbb{F}$-espaços vetoriais, pois σ_s é um automorfismo linear, resulta $\sigma_s(\mathcal{C}) = \mathcal{C}$. Além disso, podemos considerar o subgrupo gerado $\langle\{\sigma_{s=1}^{\ell}\}\rangle \subset \mathrm{PAut}(\mathcal{C})$ e temos assim uma gama de automorfismos de permutações.

Exemplo 3.2.4. Seja $\mathbb{F} = \mathbb{F}_q$ o **automorfismo de Frobenius** sobre $\mathbb{F}$ é o automorfismo linear $F : \mathbb{F} \to \mathbb{F}$, definido por, $F(\alpha) = \alpha^q$. O automorfismo F age sobre $\mathcal{A}(n_1, \ldots, n_\ell)$ do seguinte modo

$$F\left(\sum_j a_j X^j\right) = \sum_j a_j X^{q.j}$$

A aplicação F definida sobre $\mathcal{A}(n_1, \ldots, n_\ell)$ é um automorfismo linear. De fato, primeiramente, mostraremos que a aplicação

$$\begin{array}{rccc} f: & G & \to & G \\ & (i_1, \ldots, i_\ell) & \mapsto & (qi_1, \ldots, qi_\ell) \end{array}$$

é uma permutação de G. Com efeito, lembre-se que $mdc(q, n) = 1$ em que $n = n_1 \cdot \cdots \cdot n_\ell$. Note que f é bem definida e é injetiva, pois $(i_1, \ldots, i_\ell) = (j_1, \ldots, j_\ell)$ se, e somente se, $i_k \equiv j_k \pmod{n_k}$ se, e somente se, $qi_k \equiv qj_k \pmod{n_k}$ para cada $k = 1, \ldots \ell$. Isto equivale a termos $f((i_1, \ldots, i_\ell)) = f((j_1, \ldots, j_\ell)$. Também, sendo G finito, tem-se f sobrejetiva.

Assim, $f \in S_{\mathbb{Z}_{n_1}\times\ldots\times\mathbb{Z}_{n_\ell}}$. Além disso, com alguns cálculos simples, vê-se que f é um isomorfismo sobre o grupo G. Logo a extensão de f, definida por

$$\begin{array}{rccc} f^*: & \mathbb{F}G & \to & \mathbb{F}G \\ & \sum_{g\in G} a_g g & \mapsto & \sum_{g\in G} a_g f(g) \end{array}$$

é um automorfismo de $\mathbb{F}$-álgebras. Agora, note que:

$$f^*\left(\sum_{g=(j_1,\ldots,j_\ell)} a_g g\right) = \sum_{g=(j_1,\ldots,j_\ell)} a_g(qj_1,\ldots,qj_\ell)$$

Portanto, f induz F que é um automorfismo de permutação. Além disto, $F \in \mathrm{PAut}(\mathcal{C})$, para todo código abeliano $\mathcal{C}$. Para provar isto, mostraremos que $\mathcal{D}(F(\mathcal{C})) = \mathcal{D}(\mathcal{C})$ e, sendo $F(\mathcal{C})$ um código abeliano sobre $\mathcal{A}(n_1,\ldots,n_\ell)$ teremos, pelo Teorema 2.3.16, $F(\mathcal{C}) = \mathcal{C}$. Tome $i = (i_1,\ldots,i_\ell) \in \mathcal{D}(\mathcal{C})$. Então para cada $c = c(X_1,\ldots,X_\ell) \in \mathcal{C}$, tem-se que $c(\alpha^{i_1},\ldots,\alpha^{i_\ell}) = 0$. Ainda, como $qi \in \mathcal{O}(i)$, segue:

$$0 = c(\alpha^{qi_1},\ldots,\alpha^{qi_\ell}) = F(c)(\alpha^{i_1},\ldots,\alpha^{i_\ell}).$$

Da arbitrariedade de $c \in \mathcal{C}$, resulta que $i \in \mathcal{D}(F(\mathcal{C}))$. Também, sendo i tomado arbitrariamente em $\mathcal{D}(\mathcal{C})$, resulta $\mathcal{D}(\mathcal{C}) \subset \mathcal{D}(F(\mathcal{C})$. De maneira exatamente análoga, vê-se a inclusão contrária e, portanto, $\mathcal{D}(\mathcal{C}) = \mathcal{D}(F(\mathcal{C}))$.

Definição 3.2.5. *Seja $p = \sum_{j\in G} \lambda_j X^j \in \mathcal{A}(n_1,\ldots,n_\ell)$ um elemento qualquer. Definimos o **suporte** de p como sendo $supp(p) = \{j \in G : \lambda_j \neq 0\}$. Isto é, $supp(p)$ é o conjunto de todos os índices em G tais que os coeficientes associados são não nulos.*

Sejam $\mathcal{C}$ um código de comprimento ℓ e capacidade de correção κ sobre um corpo $\mathbb{F}$. Como vimos, na Definição 1.2.36, dado $s \leq \kappa$, um s-PD-conjunto para $\mathcal{C}$, relativo a um conjunto de informações $\mathcal{I}$, é um conjunto $X \subset \mathrm{PAut}(\mathcal{C})$ tal que cada conjunto de s posições de coordenadas é movido por pelo menos um elemento de X para fora de $\mathcal{I}$.

Considere o subgrupo $\Lambda := \langle\{\sigma_s\}_{s=1}^n \cup F\rangle \subset \mathrm{PAut}(\mathcal{C})$, em que σ_s e F são os automorfismos apresentados nos Exemplos 3.2.3 e 3.2.4, respectivamente. Mostraremos a existência de PD-conjuntos contidos Λ relativos ao conjunto de informações $\Gamma(\mathcal{C})^c$. A partir de agora, nos restringiremos aos códigos abelianos em duas variáveis, isto é, os códigos em $\mathcal{A}(n_1,n_2)$.

Proposição 3.2.6. *Seja $\mathcal{C} \subset \mathcal{A}(n_1, n_2)$ um código abeliano com capacidade de correção $\kappa \geq 2$ e conjunto de posições de verificação $\Gamma(\mathcal{C})$. Se $\Gamma(\mathcal{C})$ intersecta todas as q-órbitas em $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, então Λ é um 2-PD-conjunto com respeito a $\Gamma(\mathcal{C})^c$.*

Demonstração. Suponha que uma palavra $c = \sum c_{(j_1,j_2)} X_1^{j_1} X_2^{j_2} \in \mathcal{C}$ tenha sido recebida como r e que no máximo dois erros ocorreram. Considere

$$supp(e) = supp(c - r) = \{p_1, p_2\} \subset \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$$

o suporte do vetor erro e. Isto é, $p_j = (p_j^1, p_j^2))$, com $j = 1, 2$, são os índices dos coeficientes de e que são não nulos. Usando o subgrupo $\langle \sigma_1, \sigma_2 \rangle$ podemos transportar $p_1 \mapsto (0, 0) \in \Gamma(\mathcal{C})$ e $p_2 \mapsto p$ para um conveniente $p \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$. Uma vez que $\Gamma(\mathcal{C})$ intersecta todas as q-órbitas de $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, segue, existe $i \in \mathbb{N}$, tal que, $q^i p \in \Gamma(\mathcal{C})$. Assim, $F^i(0, 0) = (0, 0) \in \Gamma(\mathcal{C})$ e $\mathbb{F}^i(p) \in \Gamma(\mathcal{C})$. Portanto, Λ é um 2-PD-conjunto para $\Gamma(\mathcal{C})^c$. □

Os exemplos a seguir podem ser encontrados em [2].

Exemplo 3.2.7. Vamos projetar códigos binários corretores de até 2 erros e comprimento 45, de modo que Λ contenha um 2-PD-conjunto relativo a $\Gamma(\mathcal{C})^c$. Antes, observemos que é possível verificar, usando o programa GAP, que qualquer código abeliano, $\mathcal{C}$, com comprimento 45 e $dim(\mathcal{C}) \geq 33$ possui distância máxima $d(\mathcal{C}) \leq 4$, ou seja, se quisermos códigos abelianos com capacidade de correção de até 2 erros, devemos procurar códigos de dimensão menor ou igual a 32. Estudemos antes o caso cíclico, isto é, estudaremos os códigos abelianos de $\mathcal{A}(5, 9)$. As 2-órbitas de $\mathbb{Z}_5 \times \mathbb{Z}_9$ são

$$\mathcal{O}(0,0), \mathcal{O}(0,1), \mathcal{O}(0,3), \mathcal{O}(1,0), \mathcal{O}(1,1), \mathcal{O}(1,2)\mathcal{O}(1,3), \mathcal{O}(1,6),$$

Consideremos os códigos $\mathcal{C}_1, \ldots, \mathcal{C}_6$ de dimensão 29 com conjunto definidores:

$$\mathcal{D}(\mathcal{C}_1) = \mathcal{O}(1,2) \cup \mathcal{O}(1,6)$$
$$\mathcal{D}(\mathcal{C}_2) = \mathcal{O}(1,1) \cup \mathcal{O}(1,6)$$
$$\mathcal{D}(\mathcal{C}_3) = \mathcal{O}(1,2) \cup \mathcal{O}(1,3)$$
$$\mathcal{D}(\mathcal{C}_4) = \mathcal{O}(1,1) \cup \mathcal{O}(1,3)$$
$$\mathcal{D}(\mathcal{C}_5) = \mathcal{O}(1,0) \cup \mathcal{O}(1,2)$$
$$\mathcal{D}(\mathcal{C}_6) = \mathcal{O}(1,0) \cup \mathcal{O}(1,1).$$

Com alguns cálculos vê-se que:

$$d(\mathcal{C}_i) = 5, \forall i = 1, \ldots, 6.$$

Uma vez que,

$$\Gamma(\mathcal{C}_i) \supset \{(0,0),(0,1),(0,3),(1,0),(1,1),(1,2),(1,3),(2,3)\}$$

para cada $i = 1, \ldots, 6$. Temos, pela Proposição 3.2.6, que Λ é um 2-PD-conjunto com respeito a $\Gamma(\mathcal{C}_i)^c$ para cada $i = 1, \ldots, 6$.

Exemplo 3.2.8. Agora, construiremos um código binário não cíclico de comprimento 45 corrigindo até 2 erros. Nesse caso, consideramos todas as 2-órbitas em $\mathbb{Z}_3 \times \mathbb{Z}_{15}$, dadas por

$$\mathcal{O}(0,0), \mathcal{O}(0,1), \mathcal{O}(0,3), \mathcal{O}(0,5), \mathcal{O}(0,7), \mathcal{O}(1,0), \mathcal{O}(1,1),$$
$$\mathcal{O}(1,2), \mathcal{O}(1,3), \mathcal{O}(1,5), \mathcal{O}(1,6), \mathcal{O}(1,7), \mathcal{O}(1,10), \mathcal{O}(1,11)$$

Pode-se verificar que o código $\mathcal{C}_7$, com conjunto definidor

$$\mathcal{D}(\mathcal{C}_7) = \mathcal{O}(0,3) \cup \mathcal{O}(0,7) \cup \mathcal{O}(1,0) \cup \mathcal{O}(1,11)$$

possui dimensão 31 e $d(\mathcal{C}_7) = 6$. Logo, $\mathcal{C}_7$ é um código corretos de 2 erros. Os parâmetros para $\Gamma(\mathcal{C}_7)$ são $f[1] = 8 > f[2] = 3$ e $g[1] = 1 < g[2] = 3$ que fornecem:

$$\Gamma(\mathcal{C}_7) = \{(0,0),(0,1),(0,2),(0,3),(0,4),(0,5),(0,6),(0,7),(1,0),(2,0)\}.$$

Afirmo que $\langle \sigma_1, \sigma_2 \rangle$ é um 2-PD-conjunto com respeito a $\Gamma(\mathcal{C}_7)^c$. De fato, tome $e \in \mathcal{A}(3,5)$ um vetor erro com $supp(e) = \{p_1, p_2\} \subset \mathbb{Z}_3 \times \mathbb{Z}_{15}$ em que $p_j = (p_j^1, p_j^2)$ e $j = 1, 2$. Usando $\langle \sigma_1, \sigma_2 \rangle$ afirmo que podemos transportar $p_1 \mapsto (x_1, 0) \in \Gamma(\mathcal{C}_7)$ e $p_2 \mapsto (x_2, y_2)$ com $x_1, x_2 \in \mathbb{Z} - 3$ e $0 \leq y_2 \leq 7$. De fato, considere os seguintes casos:

1. Se $p_1^2 - p_2^2 \leq 7$. Tome $k = -p_1^2$ e veja que:

   $$\sigma_2^k(p_1) = (p_1^1, p_1^2 + k) = (p_1^1, 0) \text{ e } \sigma_2^k(p_2) = (p_2^1, p_2^2 + k) = (p_2^1, p_1^2 - p_2^2),$$

   com $p_1^2 - p_2^2 \leq 7$.

2. Se $p_1^2 - p_2^2 \geq 8$, então $p_1^2 \geq 8 + p_2^2$ implicando que $0 \leq p_2^2 \leq 7$ donde $0 \leq p_2^2 - p_1^1 \leq 7$. Fazendo $k = -p_1^2$, temos

   $$\sigma_2^k(p_1) = (p_1^1, p_1^2 + k) = (p_1^1, 0) \text{ e } \sigma_2^k(p_2) = (p_2^1, p_2^2 + k) = (p_2^1, p_2^2 - p_1^2),$$

o que justifica a afirmação. Finalmente, usando σ_1, transportamos $(x_2, y_2) \mapsto (0, y_2) \in \Gamma(\mathcal{C})$. Assim, p_1 e p_2 são transportados para fora de $\Gamma(\mathcal{C})^c$ e, portanto, $\langle \sigma_1, \sigma_2 \rangle$ é um 2-PD-conjunto relativo a este.

Agora, vejamos um caso em que Λ é um 3-PD-conjunto relativo a $\Gamma(\mathcal{C})^c$.

Proposição 3.2.9. *Seja $\mathcal{C} \subset \mathcal{A}(n_1, n_2)$ um código abeliano com capacidade de correção $\kappa \geq 3$. Se $f[1] = n_2$, $g[s_\ell] = n_1$ e $\Gamma(\mathcal{C})$ intersecta todas as q-órbitas em $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, então Λ é um 3-PD-conjunto relativo a $\Gamma(\mathcal{C})^c$.*

Demonstração. Tome $e \in \mathcal{A}(n_1, n_2)$ um vetor erro com $supp(e) = \{p_1, p_2, p_3\} \subset \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ e $p_j = (p_j^1, p_j^2)$ para $j = 1, 2, 3$. Usando $\langle \sigma_1, \sigma_2 \rangle$ transportamos $p_1 \mapsto (a_1, 0)$, $p_2 \mapsto (0, a_2)$ e $p_3 \mapsto p$ para convenientes $a_1 \in \mathbb{Z}_{n_1}$, $a_2 \in \mathbb{Z}_{n_2}$ e $p \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$. Pela hipótese e do fato que $\overline{\mathcal{D}}(\mathcal{C})$ é um conjunto restrito de representantes, existe um inteiro positivo i, de modo que $F^i(p) \in \Gamma(\mathcal{C})$, $F^i(a_1, 0) = (a_1', 0)$ e $F^i(0, a_2) = (0, a_2')$ que estão em $\Gamma(\mathcal{C})$. Portanto, Λ é um 3-PD-conjunto com respeito a $\Gamma(\mathcal{C})^c$. □

Exemplo 3.2.10. Vamos projetar códigos cíclicos binários corrigindo 3 erros, com alta dimensão e comprimento 65, de modo que Λ contenha um 3-PD-conjunto com relação a $\Gamma(\mathcal{C})$. Nesse caso, as 2-órbitas em $\mathbb{Z}_5 \times \mathbb{Z}_{13}$ são:

$$\mathcal{O}(0,0),\ \mathcal{O}(0,1),\ \mathcal{O}(1,0),\ \mathcal{O}(1,1),\ \mathcal{O}(1,2),\ \mathcal{O}(1,4),\ \mathcal{O}(1,7)$$

Consideramos os códigos $\mathcal{C}_1, \ldots, \mathcal{C}_4$, de dimensão 40, dados pelos seguintes conjuntos definidores:

$$\begin{aligned}
\mathcal{D}(\mathcal{C}_1) &= \mathcal{O}(0,0) \cup \mathcal{O}(0,1) \cup \mathcal{O}(1,1) \\
\mathcal{D}(\mathcal{C}_2) &= \mathcal{O}(0,0) \cup \mathcal{O}(0,1) \cup \mathcal{O}(1,1) \\
\mathcal{D}(\mathcal{C}_3) &= \mathcal{O}(0,0) \cup \mathcal{O}(0,1) \cup \mathcal{O}(1,4) \\
\mathcal{D}(\mathcal{C}_4) &= \mathcal{O}(0,0) \cup \mathcal{O}(0,1) \cup \mathcal{O}(1,7).
\end{aligned}$$

Vê-se que $d(\mathcal{C}_i) = 8$ para cada $1, \ldots, 4$. Além disso,

$$\{(0,0), (0,1), (1,0), (1,1), (1,2), (1,4), (1,7)\} \subset \Gamma(\mathcal{C}_i), \forall i = 1, \ldots, 4$$

Logo, pela Proposição 3.2.9, segue Λ é um 3-PD-conjunto relativo a $\Gamma(\mathcal{C})^c$.

Bibliografia

[1] J. J. Bernal, Á. del Río, and J. J. Simón. An intrinsical description of group codes. *Designs, Codes and Cryptography*, 51(3):289–300, 2009.

[2] J. J. Bernal and J. J. Simón. Information sets from defining sets in abelian codes. *IEEE transactions on information theory*, 57(12):7990–7999, 2011.

[3] J. J. Bernal and J. J. Simón. Partial permutation decoding for abelian codes. *IEEE transactions on information theory*, 59(8):5152–5170, 2013.

[4] A. Garcia and Y. Lequain. *Elementos de álgebra*. Instituto de Matemática Pura e Aplicada, 2006.

[5] C. Guneri. Artin-schreier families and 2-d cycle codes. *Doctoral Dissertation - Louisiana State University and Agricultural and Mechanical College*, 2001.

[6] A. Hefez and M. L. T. Villela. *Códigos corretores de erros*. Instituto de Matematica Pura e Aplicada, 2008.

[7] W. C. Huffman and V. Pless. Fundamentals of error-correcting codes, 2003.

[8] H. Imai. A theory of two-dimensional cyclic codes. *Information and Control*, 34(1):1–21, 1977.

[9] T. Judson. *Abstract algebra: theory and applications*. Virginia Commonwealth University Mathematics, 2009.

[10] S. Ling and C. Xing. *Coding theory: a first course*. Cambridge University Press, 2004.

[11] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*, volume 16. Elsevier, 1977.

[12] M. F. MacWilliams. Binary codes which are ideals in the group algebra of an abelian group. *Bell System Technical Journal*, 49(6):987–1011, 1970.

[13] P. A. Martin. *Grupos, corpos e teoria de Galois*. Livraria da Física, 2010.

[14] C. P. Milies and F. D. de Melo. On cyclic and abelian codes. *IEEE transactions on information theory*, 59(11):7314–7319, 2013.

[15] C. P. Milies and S. K. Sehgal. *An introduction to group rings*, volume 1. Springer Science & Business Media, 2002.

[16] S. Nagpaul. *Basic abstract algebra*. Cambridge University Press, 1994.

[17] J. J. Rotman. *An introduction to the theory of groups*, volume 148. Springer Science & Business Media, 2012.

[18] S. Sakata. On determining the independent point set for doubly periodic arrays and encoding two-dimensional cyclic codes and their duals. *IEEE Transactions on Information Theory*, 27(5):556–565, 1981.

[19] I. N. Stewart. *Galois Theory*. CRC Press, 2015.